bitdefender
TOTAL SECURITY 2008
Manuale utente

BitDefender Total Security 2008

Manuale utente

Pubblicato 2007.09.11

Avvertenze Legali

Sommario

Licenza e garanzia

SE NON SI ACCETTANO I TERMINI E LE CONDIZIONI NON INSTALLARE IL SOFTWARE. SELEZIONANDO "ACCETTO", "OK", "CONTINUA", "SI", OPPURE INSTALLANDO O UTILIZZANDO IN OGNI CASO IL SOFTWARE, STATE INDICANDO IL VOSTRO COMPLETO BENESTARE E ACCETTANDO I TERMINI DI QUESTO ACCORDO.

Questi termini ricoprono le Soluzioni e i Servizi BitDefender per gli utilizzatori Home, incluse le documentazioni relative e qualsiasi aggiornamento e rinnovo delle applicazioni rese disponibili dalla licenza acquistata o qualsiasi servizio in accordo a quanto definito nella documentazione e ogni copia di questa.

Questo accordo di Licenza è un contratto legale tra te (utente finale o individuale o entità singola) e BITDEFENDER, per l'utilizzo dei prodotti Software BITDEFENDER identificati sopra, che include il software e può includere supporti digitali, materiale stampato, e documentazione “online” oppure elettronica (qui di seguito designata come “BitDefender”), tutti protetti dalle leggi degli Stati Uniti ed internazionali sul copyright, e trattati di protezione internazionali. Mediante l'installazione, copia, o qualsiasi uso di BitDefender, accetti di essere vincolato ai termini di questo accordo. Se non accetti i termini di questo accordo, non installare ne usare BitDefender; puoi, in ogni caso, riportarlo al tuo punto vendita per il rimborso completo dell'importo versato, entro 30 giorni dall'acquisto del quale potrà essere richiesta una ricevuta.

Se non si è d'accordo con i termini che determinano il contratto di utilizzo della licenza, non installare o utilizzare BitDefender.

Licenza BitDefender. BitDefender è protetto da leggi e trattati internazionali sul copyright, così come da altre leggi e trattati sulla proprietà intellettuale. BitDefender è fornito su licenza d'uso, non venduto.

CONCESSIONE DI LICENZA. BITDEFENDER concede,solamente all'utente che l'ha acquistata e non a terzi, la presente licenza non esclusiva, limitata e non trasferibile, a utilizzare BitDefender.

APPLICAZIONE DEL SOFTWARE. Si può installare e usare BitDefender, su quanti computers è necessario ma limitatamente al numero totale di utenti autorizzati dalla licenza. E' possibile fare una copia addizionale di back-up.

LICENZA UTENTE DESKTOP. Questa licenza si applica al software BitDefender che può essere installato su un computer singolo e che non fornisce servizi di rete. Ogni utente principale può installare questo software su un computer singolo e può eseguire

una copia aggiuntiva per il backup su un dispositivo diverso. Il numero di utenti principali consentito è il numero di utenti della licenza.

PERIODO DI LICENZA. Il periodo di validità, avrà inizio dalla data in cui viene eseguita l'installazione, la copia, o quando viene usato in qualche modo, per la prima volta, BitDefender, e continuerà solamente sul computer dove è stato originariamente installato.

SCADENZA. Il prodotto cesserà di compiere le sue funzioni immediatamente dopo la scadenza della licenza.

UPGRADE (AGGIORNAMENTO). Se BitDefender è identificato come un upgrade, per usarlo devi essere stato autorizzato precedentemente ad utilizzare un prodotto classificato da BITDEFENDER come idoneo all' aggiornamento. Un prodotto BitDefender classificato come upgrade, sostituisce o complementa il prodotto originariamente installato e idoneo. Puoi usare il prodotto aggiornato esclusivamente in conformità con i termini di questo Accordo di Licenza. Se BitDefender è l' upgrade di un componente di un pacchetto di programmi software, dato in licenza come un solo prodotto, può essere utilizzato e trasferito solamente come parte integrante di questo pacchetto e non può essere separato per l'utilizzo su più di un computer.

COPYRIGHT. Tutti i diritti, titoli, e interessi derivati da o verso BitDefender e tutti i diritti di copyright derivati da o verso BitDefender (includendo ma non limitando qualsiasi immagine, fotografia, logo, animazione, video, audio, musica, testo e "applets" incorporati nel BitDefender) il materiale stampato allegato e qualsiasi copia di BitDefender sono proprietà della BITDEFENDER. BitDefender è protetto dalle leggi di copyright e da quanto previsto dai trattati internazionali. Di conseguenza, BitDefender deve essere considerato come qualunque altro materiale protetto da copyright ad eccezione del fatto che è possibile installare BitDefender su un singolo computer conservando l'originale esclusivamente per scopi di backup o archiviazione. Non è permessa la copia o riproduzione del materiale stampato e allegato al prodotto o supporto BitDefender. In tutte le copie create indipendentemente dal supporto o formato in cui vi sia BitDefender, è necessario riprodurre ed includere tutte le note copyright in formato originale. Non è permesso noleggiare a terzi, vendere, dare in leasing, la licenza di BitDefender. Non è permesso smontare, raggruppare, disassemblare, creare lavori derivati, modificare, tradurre né fare alcun tentativo per scoprire, individuare, il codice fonte di BitDefender.

GARANZIA LIMITATA. BITDEFENDER garantisce che il supporto con il quale viene distribuito BitDefender è esente da difetti per un periodo di trenta giorni dalla data in cui viene consegnato. In caso di difettosità riscontrate, BITDEFENDER, a sua discrezione, potrà sostituire il supporto, oppure rimborsare l'importo pagato per l'acquisto, a fronte di una ricevuta. BITDEFENDER non garantisce che BitDefender

sarà sempre privo di errori o che gli errori verranno comunque corretti. BITDEFENDER non garantisce che BitDefender soddisferà le necessità dell'utilizzatore. BITDEFENDER CON LA PRESENTE NEGA QUALSIASI ALTRA GARANZIA PER BITDEFENDER, SIA ESPLICITA CHE IMPLICITA. LA SUDDETTA GARANZIA E' ESCLUSIVA E SOSTITUISCE TUTTE LE ALTRE GARANZIE, SIA ESPLICITE CHE IMPLICITE, INCLUDENDO LE GARANZIE DI COMMERCIABILITA', DI ADEGUAMENTO AD UN PROPOSITO PARTICOLARE, O DI NON INFRAZIONE. QUESTA GARANZIA CONCEDE DIRITTI LEGALI SPECIFICI CHE POSSONO VARIARE DA STATO A STATO.

ECCETTO PER QUANTO CHIARAMENTE SOTTOLINEATO IN QUESTO ACCORDO, ESPRESSAMENTE O IMPLICITAMENTE, RISPETTO AI PRODOTTI, AI MIGLIORAMENTI, ALLA MANUTENZIONE O AL SUPPORTO AD ESSI RELATIVI, O A QUALSIASI ALTRO MATERIALE (TANGIBILE O INTANGIBILE) O SERVIZIO FORNITO DA QUESTI. BITDEFENDER QUI DISCONOSCE ESPRESSAMENTE QUALSIASI GARANZIA E CONDIZIONE IMPLICITA, INCLUSO, SENZA LIMITAZIONE, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, APPROPRIATEZZA PER UNO SCOPO PARTICOLARE, TITOLO, NON INTERFERENZA, ACCURATEZZA DEI DATI, ACCURATEZZA DEL CONTENUTO INFORMATIVO, INTEGRAZIONE DEL SISTEMA, E NON VIOLAZIONE DEI DIRITTI DI TERZE PARTI ATTRAVERSO IL FILTRO, LA DISABILITAZIONE, O LA RIMOZIONE DI TALE SOFTWARE, SPYWARE, ADWARE, COOKIE, E-MAIL, DOCUMENTI, PUBBLICITÀ O SIMILI, DI TERZE PARTI, CHE SI ORIGININO DA STATUTO, LEGGE, CORSO DI TRATTATIVE, COSTUMI E PRATICA, O USI DEL COMMERCIO.

DECLINAZIONE DELLE RESPONSABILITA' DI DANNI. Chiunque utilizzi, provi oppure valuti BitDefender, si assume tutto il rischio della qualità e delle prestazioni di BitDefender. In nessun caso BITDEFENDER sarà ritenuta responsabile di qualunque danno di qualsiasi tipo, inclusi senza limitazioni, danni diretti o indiretti derivati dall' utilizzo, o la consegna di BitDefender, anche nel caso in cui BITDEFENDER sia informata dell'esistenza o la possibilità che tali danni possano verificarsi. ALCUNI STATI NON CONSENTONO LA LIMITAZIONE O L' ESCLUSIONE DI RESPONSABILITA' PER DANNI ACCIDENTALI O CONSEGUENTI, IN QUEL CASO LA LIMITAZIONE O ESCLUSIONE SOPRA INDICATA NON POTRA' ESSERE APPLICATA. IN NESSUN CASO COMUNQUE, LA RESPONSABILITA' DI BITDEFENDER POTRA' ECCEDERE IL PREZZO CHE PAGATO PER L'ACQUISTO DI BITDEFENDER. Le restrizioni e limitazioni fissate saranno applicate indipendentemente dal modo in cui si accetta di usare, valutare o provare BitDefender.

AVVISO IMPORTANTE AGLI UTENTI. AVVISO IMPORTANTE AGLI UTENTI. QUESTO SOFTWARE NON E ESENTE DA EVENTUALI DIFETTI PROVOCATI ANCHE DALL'UTILIZZO DELLO STESSO, E NON E' STATO PROGETTATO NE'

DESTINATO ALL'USO IN AMBIENTI PERICOLOSI CHE RICHIEDANO OPERAZIONI O ATTIVITA' IN MANCANZA DI SICUREZZA. QUESTO SOFTWARE NON E' ADATTO ALL'USO IN OPERAZIONI DI NAVIGAZIONE AEREA, NELLE ISTALLAZIONI NUCLEARI, NEI SISTEMI DI COMUNICAZIONE, SISTEMI DI ARMAMENTO, SISTEMI DI RESPIRAZIONE ASSISTITA DIRETTA O INDIRETTA, CONTROLLO DEL TRAFFICO AEREO O QUALUNQUE APPLICAZIONE, ISTALLAZIONE, DOVE L'ERRORE POSSA PROVOCARE MORTE, LESIONI FISICHE GRAVI, O DANNI ALLA PROPRIETA'.

GENERALE. Questo accordo sarà regolato dalle leggi della Romania e dai regolamenti e trattati internazionali sul diritto d'autore. La giurisdizione esclusiva e la sede di decisione per qualsiasi disputa che sorga al di fuori di questi Termini di Licenza sarà in capo ai tribunali della Romania.

I prezzi, i costi e le tasse per l'uso di BitDefender sono soggetti a variazione senza preventiva notifica.

Nel caso di invalidità di qualsiasi previsione di questo Accordo, l'invalidaità non avrà effetto sulla validità delle porzioni residue di questo Accordo.

BitDefender e i lochi BitDefender sono marchi registrati di BITDEFENDER. Tutti gli altri marchi registrati utilizzati nel prodotto o nei materiali associati sono di proprietà dei rispettivi titolari.

La licenza terminerà immediatamente senza notifica se si infrange uno qualsiasi dei suoi termini e condizioni. Non si ha diritto ad alcun rimborso da BITDEFENDER o da qualsiasi rivenditore di BitDefender come risultato della cessazione. I termini e le condizioni che riguardano la riservatezza e le restrizioni d'uso resteranno in vigore anche dopo qualsiasi cessazione.

BITDEFENDER può revisionare questi Termini in qualsiasi momento e i termini revisionati si applicheranno automaticamente alle versioni corrispondenti del Software distribuito con i termini revisionati. Se qualsiasi parte di questi Termini è giudicata nulla o non applicabile, ciò non avrà effetto sulla validità del resto dei Termini, che resteranno validi ed applicabili.

In caso di controversia o inconsistenza tra le traduzioni di questi Termini nelle altre lingue, prevarrà la versione inglese emessa da BITDEFENDER.

Contattare BITDEFENDER, al n.5 di via Fabrica de Glucoza, 72322-Sector 2, Bucarest, Romania, o al N. di Tel. : 40-21-2330780 o di Fax: 40-21-2330763, indirizzo e-mail: office@bitdefender.com.

Prefazione

Questa Guida è destinata a tutti gli utenti che hanno scelto **BitDefender Total Security 2008** come la soluzione di sicurezza per i loro personal computers. L'informazione presentata in questo manuale non è indirizzata solo agli esperti di computer, ma anche a chiunque sia in grado di lavorare con Windows.

Questa guida, descrive **BitDefender Total Security 2008**, la Società e il Team che lo ha sviluppato, inoltre vi guiderà attraverso il processo di installazione, spiegandovi come configurarlo. Troverete come utilizzare **BitDefender Total Security 2008**, come aggiornarlo, testarlo e personalizzarlo. Imparerete come ottenere il massimo da BitDefender.

Vi auguriamo una lettura gradevole e utile.

1. Convenzioni usate in questo manuale

1.1. Convenzioni tipografiche

Nel libro vengono usati diversi stili di testo per una buona leggibilità. L'aspetto e il significato è presentato nella tabella sottostante.

Aspetto	Descrizione
`sample syntax`	Gli esempi sintattici vengono scritti con caratteri `monospazio`.
http://www.bitdefender.com	I link URL indirizzano su ubicazioni esterne, su server http o ftp.
support@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo per informazioni sui contatti.
«Prefazione» (p. xiii)	Questo è un link interno, che indirizza verso documenti contenuti nel manuale.
`filename`	File e directory (cartelle) vengono scritte utilizzando fonti `monospazio`.
option	Tutte le opzioni del prodotto vengono evidenziate usando caratteri in **grassetto**.

Aspetto	Descrizione
`sample code listing`	La lista dei codici è scritta con caratteri `monospazio`.

1.2. Avvertenze

Le avvertenze appaiono in note di testo, segnalate graficamente, portando alla tua attenzione informazioni addizionali relative al paragrafo corrente.

Nota
La nota è una breve osservazione. Anche se è possibile ometterla, può indicare informazioni utili come una caratteristica specifica o un link verso argomenti relazionati.

Importante
Questa richiede attenzione, è sconsigliato saltarla. Solitamente contempla informazioni non critiche ma importanti.

Avvertimento
Questa è un'informazione critica che deve essere trattata con estrema cautela. Seguendone le indicazioni si eviteranno eventualità negative. Dovrebbe essere letta e compresa in quanto è la descrizione di qualcosa di estremamente rischioso.

2. Struttura del manuale

Il manuale è composto da diverse parti contenenti gli argomenti importanti. Inoltre, viene anche fornito un glossario per chiarire alcuni termini tecnici.

Installazione. Istruzioni passo-passo per installare BitDefender su una postazione di lavoro (workstation). Questa è una guida esaustiva per l' installazione di **BitDefender Total Security 2008**. Iniziando con i prerequisiti per una installazione con successo, sarete guidati attraverso tutto il processo. Al termine, è descritta la procedura di disinstallazione nel caso in cui abbiate la necessità di rimuovere BitDefender.

Amministrazione di base. Descrizione dell'amministrazione di base e manutenzione di BitDefender.

Amministrazione della Sicurezza Avanzata. Una presentazione dettagliata delle capacità di sicurezza fornite da BitDefender. I capitoli spiegano in dettaglio tutte le opzioni del console delle impostazioni avanzate. Vi spieghiamo come configurare ed utilizzare tutti i moduli di BitDefender in modo da proteggere efficacemente il vostro

computer da ogni tipo di minaccia (malware, spam, hackers, contenuto inappropriato ed altro).

Amministrazione Avanzata del Backup. Descrizione delle impostazioni avanzate di backup. Qui imparerete come impostare ed eseguire operazoni backup, recupero e masterizzazione.

BitDefender Rescue CD. Descrizione di BitDefender Rescue CD. Aiuta a capire e utilizzare le funzioni del CD di avvio.

Ottenere aiuto. Dove cercare e ottenere un aiuto in caso di difficoltà. E' inclusa anche una sezione FAQ (Domande frequenti).

Glossario. Il glossario cerca di spiegare alcuni termini tecnici e poco comuni che troverete tra le pagine di questo documento.

3. Richiesta di commenti

Vi invitiamo ad aiutarci a migliorare questo manuale. Abbiamo provato e verificato tutte le informazioni contribuendo con il massimo delle nostre risorse, ma se trovare errori vi invitiamo a darcene una immediata comunicazione. Per aiutarci a fornire la migliore documentazione possibile, non esitate a scriverci, comunicando i vostri consigli.

Informateci inviando una e-mail a documentation@bitdefender.com.

Importante

Per una comunicazione efficiente, vi invitiamo a scrivere i vostri documenti e le e-mails in lingua Inglese.

Installazione

1. Installazione di BitDefender Total Security 2008

La sezione **Installazione di BitDefender Total Security 2008** di questa guida all'utente contiene i seguenti argomenti:

1.1. Requisiti del sistema

Per assicurare un funzionamento appropriato del prodotto, verificare, prima dell'installazione, che sul vostro computer giri uno dei seguenti sistemi operativi e che vi siano i seguenti requisiti di sistema:

- Piattaforma operativa: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (o superiore)
- Client e-mail supportati: Microsoft Outlook 2000 / 2003 / 2007; Microsoft Outlook Express; Microsoft Windows Mail; Thunderbird 1.5 e 2.0

Windows 2000

- Processore 800 MHz o superiore
- Minimo 256 MB di memoria RAM (consigliati 512 MB)
- Minimo 60 MB di spazio disponibile su hard disk

Windows XP

- Processore 800 MHz o superiore
- Minimo 256 MB di Memoria RAM (consigliati 1 GB)
- Minimo 60 MB di spazio disponibile su hard disk

Windows Vista

- Processore 800 MHz o superiore

- Minimo 512 MB di Memoria RAM (raccomandati 1 GB)
- Minimo 60 MB di spazio disponibile su hard disk

BitDefender Total Security 2008 può essere scaricato per una valutazione all'indirizzo:http://www.bitdefender.com il sito di BITDEFENDER corporate, dedicato alla sicurezza dei dati.

1.2. Fasi per l'installazione

Individuare il file di setup e cliccare due volte. Verrà lanciato l'assistente che vi guiderà attraverso il processo di setup:

Prima di lanciare l'assistente di setup, BitDefender controllerà la disponibilità di versioni più recenti del pacchetto di installazione. Se ci fosse una versione più recente disponibile, vi verrà proposto di scaricarla. Cliccare su **Sì** per scaricare la versione più recente oppure **No** per continuare con l'installazione della versione disponibile nel file di setup.

Fasi per l'installazione

Seguire questi passi per installare BitDefender Total Security 2008:

1. Selezionare **Avanti** per continuare oppure **Cancella** se si desidera interrompere l'installazione.
2. Selezionare **Avanti**.

   BitDefender Total Security 2008 vi avverte se avete altri prodotti antivirus installati sul vostro computer. Selezionare **Rimuovi** per disinstallare il corrispondente prodotto. Se si desidera continuare senza rimuovere i prodotti rilevati, selezionare **Avanti**.

Avvertimento
Si raccomanda di disinstallare qualsiasi altro prodotto antivirus precedentemente installato. Infatti due o più antivirus sulla stessa macchina potrebbero rendere il sistema inutilizzabile.

3. Vi preghiamo di leggere il Contratto di Licenza, e selezionare **Accetto le clausole del Contratto di Licenza** quindi selezionare **Avanti**. Se non siete d'accordo con le condizioni del contratto, selezionare **Cancella**. In questo caso abbandonerete il processo di installazione e uscirete dal setup.
4. Per default, BitDefender Total Security 2008 verrà installato in `C:\Program Files\BitDefender\BitDefender 2008`. Se si desidera modificare il percorso d'installazione, fare click su **Sfoglia**, quindi selezionare, la cartella dove si desidera installare BitDefender Total Security 2008.

   Selezionare **Avanti**.
5. Selezionare le opzioni relative al processo di installazione. Alcune di loro verranno selezionate di default:
   - **Aprire il file readme** - per aprire il file readme al termine dell'installazione.
   - **Inserire un collegamento sul desktop** - per inserire un collegamento a BitDefender Total Security 2008 sul desktop, al termine dell' installazione.
   - **Espellere CD al termine dell'installazione** - per che il CD venga espellito al termine dell'installazione; questa opzione apparirà se installerete il prodotto dal CD.
   - **Disattiva il Firewall di Windows** - per disattivare il Firewall di Windows.

Importante
Vi raccomandiamo di disabilitare il Firewall di Windows poichè BitDefender Total Security 2008 include già un firewall avanzato. Far girare due firewall sullo stesso computer può causare problemi.

   - **Disattiva Windows Defender** - per disattivare Windows Defender; questa opzione compare slo su Windows Vista.

Selezionare **Installa** per iniziare l'installazione del prodotto.

Importante
Durante il processo di installazione apparirà un assistente. L'assistente vi aiuterà a registrare il vostro **Sicurezza Totale BitDefender 2008**, a creare un account BitDefender e ad impostare BitDefender per eseguire importanti compiti di sicurezza. Completare il processo di configurazione assistita per accedere al passo successivo.

6. Selezionare **Termina** per completare l'installazione del prodotto. Se avete accettato le impostazioni di default per il percorso di installazione, verrà creata una nuova cartella chiamata `BitDefender` in `Programmi` che contiene la sottocartella `BitDefender 2008`.

Nota
Potrebbe essere richiesto di riavviare il sistema in modo che l'assistente di setup completi il processo di installazione.

1.3. Assistente per il Setup iniziale

Durante il processo di installazione comparirà un assistente. L'assistente vi aiuterà a registrare il vostro **Sicurezza Totale BitDefender 2008**, a creare un account BitDefender e ad impostare BitDefender per eseguire importanti compiti per la sicurezza.

Completare il processo non è obbligatorio; in ogni caso vi raccomandiamo di farlo per guadagnare tempo e assicurare il vostro sistema prima che Sicurezza Totale BitDefender 2008 sia installato.

1.3.1. Passo 1/6 - Registrazione di BitDefender Total Security 2008

Registrazione

Scegliere **Registra il prodotto** per registrare **BitDefender Total Security 2008**. Digitare la chiave licenza nel campo **Inserisci la nuova chiave**.

Per continuare a provare il prodotto, selezionare **Continuare a provare il prodotto**.

Selezionare **Avanti**.

1.3.2. Passo 2/6 - Creare un Account BitDefender

Creazione Account

Non possiedo un account BitDefender

Per beneficiare del supporto tecnico gratuito di BitDefender e di altri servizi gratuiti dovete creare un account. Selezionare **Creare un nuovo Account BitDefender** e fornire le informazioni richieste. I dati che fornite qui resteranno riservati.

Nota
Se desiderate creare un account più tardi, selezionare l'opzione corrispondente.

Digitate un indirizzo e-mail valido nel campo **E-mail**. Pensate ad una password e digitatela nel campo **Password**. Confermate la password nel campo **Digitare nuovamente la password**. Utilizzare l'indirizzo e-mail e la password per identificarvi al vostro account alla pagina http://myaccount.bitdefender.com.

Nota
La password deve essere lunga almeno quattro caratteri.

Riempite con il vostro nome e cognome, e selezionate il paese in cui risiedete.

Per creare un account con successo dovete prima attivare il vostro indirizzo e-mail. Controllate il vostro indirizzo e-mail e seguite le istruzioni nella e-mail spedita dal servizio di registrazione BitDefender.

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

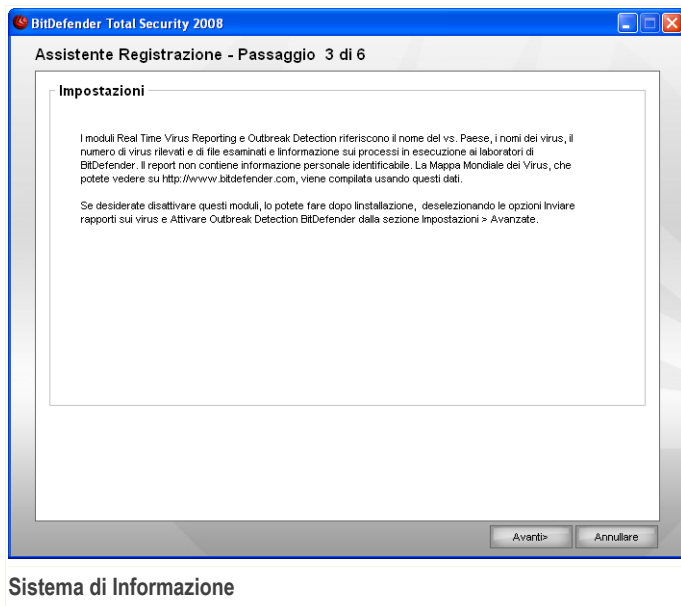
Ho già un account BitDefender

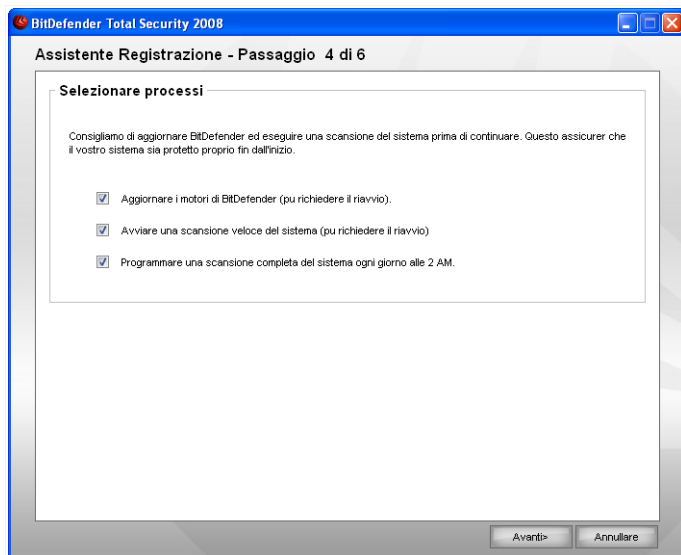
Se avete già un account attivo, fornite l'indirizzo e-mail e la password del vostro account. Se fornite una password non corretta, sarete avvisati di digitarla nuovamente quando cliccate su **Avanti**. Cliccate su **Ok** per inserire di nuovo la password o su **Annulla** per uscire dall'assistente.

Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

1.3.3. Passo 3/6 - Imparare riguardo a RTVR

Sistema di Informazione

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

1.3.4. Passo 4/6 – Seleziona l’azione

Selezione azioni

Impostare BitDefender Total Security 2008 per eseguire importanti compiti per la sicurezza del vostro sistema.

Sono disponibili le seguenti opzioni:

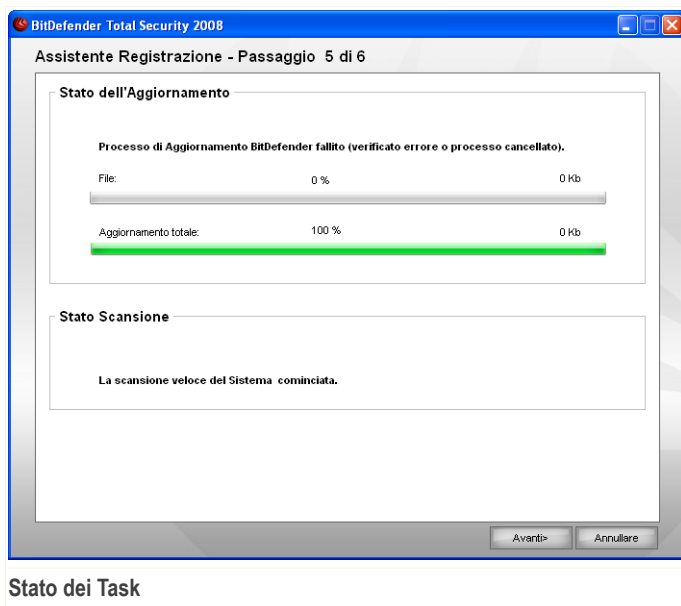
- **Aggiornamento motori BitDefender (può richiedere il riavvio)** - durante il prossimo passo, verrà eseguito un aggiornamento dei motori BitDefender per proteggere il vostro computer contro le ultime minacce.
- **Eseguite una scansione rapida del sistema (può richiedere il riavvio)** - durante il prossimo passo, verrà eseguita una scansione rapida del sistema per consentire a BitDefender di assicurarsi che i vostri file nelle cartelle di`Windows` e `File di Programma` non siano infetti.
- **Eseguire una scansione completa del sistema ogni giorno alle 2 AM** - esegue una scansione completa del sistema ogni giorno alle 2 AM.

Importante
Vi raccomandiamo di abilitare queste opzioni prima di passare al passo successivo per assicurare la sicurezza del vostro sistema.

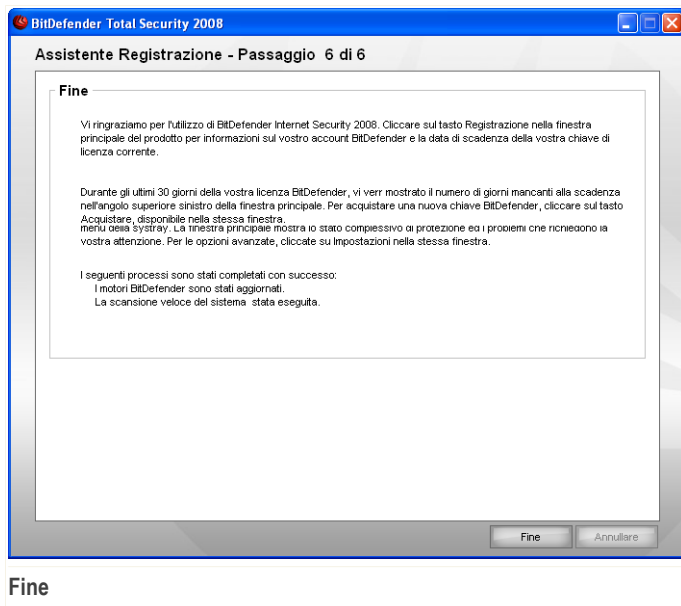
Se selezionate solo l'ultima opzione o nessuna opzione, salterete al passo successivo.

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

1.3.5. Passo 5/6 – Attendere il Completamento dei Compiti

Stato dei Task

Attendere che i compiti siano completati. Potete vedere lo stato dei compiti selezionati nel passo precedente.

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

1.3.6. Passaggio 6/6 - Sommario

Fine

Questo è l'ultimo passo del processo di configurazione.

Selezionare **Fine** per completare la configurazione e continuare con il processo di installazione.

1.4. Upgrade

L'Upgrade può essere eseguito in uno dei seguenti modi:

- **Installare senza rimuovere la versione precedente – solo per la versione 8 o superiore, escluso Internet Security.**

  Fare doppio click sul file di setup e seguire il processo descritto nella sezione *«Fasi per l'installazione»* (p. 3).

Importante
Durante il processo di installazione apparirà un messaggio di errore causato dal `servizio Filespy`. Cliccare **OK** per continuare l'istallazione.

- **Disinstallare la versione precedente ed installare quella nuova – per tutte le versioni BitDefender**

  Prima di si deve rimuovere la versione precedente, quindi riavviare il computer ed installare la nuova come descritto nella sezione «*Fasi per l'installazione*» (p. 3).

Importante
Prima di eseguire l' aggiornamento upgrade da BitDefender v8 o superiore, consigliamo di salvare le impostazioni di BitDefender, l'elenco Amici e l'elenco Spammers. Sarà possibile caricarli dopo che il processo di upgrade sarà stato completato.

1.5. Riparare o Rimuovere BitDefender

Se si desidera riparare o rimuovere **Sicurezza Totale BitDefender 2008**, selezionare dal menu di avvio di Windows: **Start** → **Programmi** → **BitDefender 2008** → **Riparare o Rimuovere**.

Verrà richiesto di confermare la vostra scelta, facendo un click su **Avanti**. Apparirà una nuova finestra dove potrete selezionare:

- **Riparare** - per re-installare tutte le componenti del programma installate dal setup precedente.

Importante
Prima di riparare il prodotto, consigliamo di salvare l'elenco degli Amici e l'elenco degli Spammers. Potete inoltre salvare le impostazioni di BitDefender ed il database Bayesiano. Una volta completato il processo di riparazione, si potranno ricaricare.

  Scegliendo di riparare BitDefender, la seguente nuova finestra comparirà. Selezionare **Riparare** per iniziare il processo di riparazione.

  Riavviare il computer quando venga richiesto, e quindi selezionare **Installare** per reinstallare Sicurezza Totale BitDefender 2008.

  Una volta completato il processo di installazione, apparirà una nuova finestra. Selezionare **Termina**.

- **Rimuovi** - per rimuovere tutte le componenti installate.

Nota
Vi consigliamo di scegliere **Rimuovere** per una reinstallazione pulita.

Scegliendo di rimuevere BitDefender, apparirà una nuova finestra.

Importante

Rimuovendo BitDefender, non sarete più protetti da virus, spyware e hacker. Se desiderate che Windows Firewall e Windows Defender (solo su Windows Vista) vengano attivati dopo aver disinstallato BitDefender, selezionare la caselle corrispondenti.

Selezionare**Rimuovere** per iniziare la rimozione di Sicurezza Totale BitDefender 2008 dal vostro computer.

Durante il processo di rimozione vi verrà chiesto di darci il vostro feedback. Vi preghiamo di fare click su **OK** per ricevere un sondaggio on line, consistente in non più di cinque brevi domande. Se non si desidera ricevere il sondaggio, fare click su **Annulla**.

Una volta completato il processo di rimozione, apparirà una nuova finestra. Selezionare **Termina**.

Nota
Al termine del processo di disinstallazione, consigliamo di cancellare la cartella `BitDefender` dei `Program Files`.

Si è verificato un errore durante la rimozione di BitDefender

Se si fosse verificato un errore durante la rimozione di BitDefender, il processo di rimozione verrà interrotto ed apparirà una nuova finestra. Selezionare**Eseguire tool di disinstallazione** per assicurarsi che BitDefender sia stato completamente rimosso. Il tool di disinstallazione rimuoverà tutti i file e chiavi di registro che non siano stati rimossi durante il processo automatico di rimozione.

Amministrazione di base

2. Iniziando

Una volta che avrete installato BitDefender il vostro computer sarà protetto. Potete aprire il Centro di Sicurezza di BitDefender per controllare lo stato di sicurezza del sistema, prendere misure preventive o configurare completamente il prodotto in qualsiasi momento.

Per accedere al Centro di Sicurezza BitDefender, usare il menu di Avvio di Windows, seguendo il percorso **Avvio** → **Programmi** → **BitDefender 2008** → **Sicurezza Totale BitDefender 2008** o più velocemente cliccando due volte sull' **icona BitDefender** dalla barra delle applicazioni (in basso a destra).

Centro di Sicurezza BitDefender

Il Centro di Sicurezza BitDefender contiene due aree:

- L'area **Stato**: contiene informazioni e vi aiuta nella risoluzione delle vulnerabilità della sicurezza del vostro computer. Potete facilmente osservare quanti problemi potrebbero colpire il vostro computer. Cliccando sul corrispondente tasto rosso **Risolvere tutti i problemi** le vulnerabilità del vostro computer verranno subito

risolte oppure verrete guidati per risolverle facilmente. Nello stesso tempo, sono disponibili quattro tasti di stato corrispondenti a quattro categorie di sicurezza. I tasti di stato in verde indicano che non c'è nessun rischio. I tasti in giallo o in rosso indicano rischi di sicurezza medi o alti. Per risolverli cliccare sul tasto giallo/rosso e quindi i tasti **Risolvere**, uno per uno oppure il tasto **Risolvere tutti adesso**. Il Grigio indica una componente non configurata.

- L'area **Funzioni Veloci**: vi aiuta a prendere misure preventive essenziali per mantenere sicuro il vostro sistema e proteggere i vostri dati. Esso consiste in tre sezioni corrispondenti a tre tipi di azioni di sicurezza. Qui potete aggiornare il vostro prodotto, esaminare il vostro computer, eseguire backup o recuperare i vostri dati, deframmentare il vostro disco, pulire i file temporanei di Internet e i cookies, cancellare e restaurare il registro, trovare file duplicati, così come eliminare file in modo sicuro.

Inoltre, il Centro di Sicurezza di BitDefender contiene diversi collegamenti utili.

Link	*Descrizione*
Comprare	Apre una pagina dalla quale potete acquistare il prodotto.
Il mio Account	Apre la pagina del vostro account BitDefender.
Registrare	Apre l'assistente per la registrazione.
Aiuto	Apre il file di aiuto.
Supporto	Apre la pagina web di supporto di BitDefender
Impostazioni	Apre il console delle impostazioni avanzate.
Storia	Apre una finestra con la storia di BitDefender; eventi.

Per gestire l'intero prodotto più velocemente, potete anche utilizzare l'icona di BitDefender presente nella barra delle applicazioni.

Menù Contestuale

Se fate doppio click su questa icona, si aprirà il Centro di Sicurezza di BitDefender. Inoltre, cliccando col tasto destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto BitDefender.

- **Mostrare** - apre il il Centro di Sicurezza di BitDefender.
- **Aiuto** - apre il file di aiuto.
- **Info** - apre la pagina web di BitDefender.
- **Risolve tutti i problemi** - vi aiuta a rimuovere tutte le vulnerabilità di sicurezza.
- **Attivare Modalità Gioco** - disattiva allarmi e pop-up ed imposta il livello di protezione in tempo reale come tollerante. Anche il Firewall BitDefender verrà impostato su **Autorizzare tutti**.
- **Aprire impostazioni avanzate** - consente l'accesso al console delle impostazioni avanzate.
- **Uscire** - termina l'applicazione.

2.1. Scansione Manuale di BitDefender

Se volete esaminare velocemente una certa cartella, potete usare la Scansione Manuale di BitDefender.

Per accedere alla Scansione Manuale BitDefender utilizzare il menu Avvio di Windows, seguendo il percorso **Avvio** → **Programmi** → **BitDefender 2008** → **Scansione Manuale di BitDefender**

Tutto quello che dovete fare è sfogliare le cartelle, selezionare quella desiderata e cliccare su **OK**.

3. Stato di Sicurezza

Lo stato della sicurezza mostra una lista delle vulnerabilità di sicurezza del vostro computer organizzata sistematicamente e gestibile facilmente. Sicurezza Totale BitDefender 2008 vi informerà ogni volta che un problema potrà colpire la sicurezza del vostro computer.

Ci sono quattro tasti di stato di sicurezza:

- **SICUREZZA**
- **DEI GENITORI**
- **BACKUP**
- **TUNEUP**

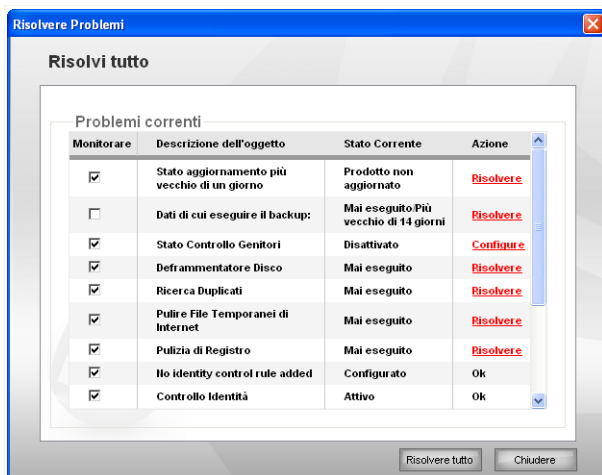
Nello stesso tempo, sulla sinistra potrete vedere il numero dei problemi che colpiscono la sicurezza del vostro sistema, ed un tasto rosso **Risolvere Tutti i Problemi**.

I quattro tasti di stato vengono visualizzati in verde, giallo, rosso o grigio, a seconda del livello corrente di protezione.

- **Verde** indica un livello basso di rischio di sicurezza per il vostro computer.
- **Giallo** indica un livello medio di rischio di sicurezza per il vostro computer.
- **Rosso** indica un livello alto di rischio di sicurezza per il vostro computer.
- **Grigio** indica una componente non configurata.

La risoluzione dei problemi di sicurezza non richiede sforzo alcuno e può farsi con un semplice click sul tasto **Risolvere tutti i problemi**.

Verrà visualizzata una lista di problemi di sicurezza ed una breve descrizione del loro stato.

Per risolvere solo un particolare problema, cliccare sul corrispondente tasto**Risolvere**. Verrà risolto subito oppure dopo che avrete seguito i passi dell'assistente. Se si decide di risolverli tutti, cliccare sul tasto **Risolvere tutti adesso** e seguire i passi dell'assistente corrispondente.

Problemi di Sicurezza

Per risolvere i problemi più tardi, cliccare su **Chiudere**.

Importante
Per ogni problema c'è una casella, selezionata per default. Se non si desidera che un problema specifico venga tenuto in conto per calcolare il rischio di sicurezza, deselezionare la casella corrispondente. Vi preghiamo di utilizzare questa opzione con cautela, poichè è molto facile aumentare il rischio al quale verrà esposto il vostro computer.

3.1. Tasto Stato di Sicurezza

Se il tasto di stato di sicurezza è verde non c'è niente di cui preoccuparsi. Invece, se il tasto è giallo, rosso o grigio, il vostro computer è esposto ad un alto o medio rischio di sicurezza.

Il colore dei tasti di stato può cambiare, non solo quando si configurano le impostazioni che riguardano la sicurezza del vostro computer, ma anche quando si dimentica di eseguire delle funzioni importanti. Ad esempio, se è da tempo che è stata eseguita l'ultima scansione del vostro sistema, il tasto di stato della sicurezza sarà giallo. Se è da tanto tempo, sarà rosso.

La tabella sotto vi fornirà l'informazione su gli elementi tenuti in conto per il calcolo del rischio di sicurezza.

Problema	Colore
L'utima scasione del sistema è stata eseguita tempo fa	Giallo
L'utima scasione del sistema è stata eseguita tanto tempo fa	Rosso
La protezione in tempo reale è disattivata	Rosso
Il livello di protezione antivirus è impostato come tollerante	Giallo
La protezione della privacy è disattivata.	Rosso
Il firewall è disattivato	Rosso
La modalità cautela è disattivata	Rosso
La connessione wireless non è stata resa sicura	Rosso
L'aggiornamento automatico è disattivato	Rosso
L'ultimo aggiornamento è di un giorno fa.	Rosso
L'antispam è disattivato	Grigio

Per risolvere i problemi, vi invitiamo a seguire questi passaggi:

1. Cliccare sul tasto stato di sicurezza.
2. Cliccare sul tasto **Risolvere** per risolverli uno alla volta oppure il tasto**Risolvere tutti adesso** per risolverli tutti inmediatamente.
3. Se un problema non venisse risolto subito, seguire i passaggi dell'assistente per risolverlo.

3.2. Tasto Stato del Controllo Genitori

Se il tasto stato di sicurezza è verde, il Controllo Genitori è attivo. Se è grigio, è disattivato.

Per attivare il Controllo Genitori, cliccare sul corrispondente tasto di stato e quindi cliccare su **Configurare**.

3.3. Tasto Stato del Backup

Se il tasto di stato del backup è verde, non c'è niente di cui preoccuparsi. Altrimenti, se il tasto è giallo o rosso, il vostro computer è esposto ad un rischio di sicurezza medio o alto.

Il colore dei tasti di stato può cambiare, non solo quando configurate le impostazioni che potrebbero colpire la sicurezza del vostro computer, ma anche quando dimenticate di eseguire funzioni importanti.

Per esempio, se non avete eseguito un backup dei dati del vostro computer da molto tempo, lo stato sarà rosso.

La tabella sotto vi fornirà l'informazione su gli elementi tenuti in conto per il calcolo del rischio di sicurezza.

Problema	Colore
L'ultimo backup dei dati è vecchio	Giallo
L'ultimo backup dei dati è molto vecchio	Rosso

Per risolvere i problemi, vi invitiamo a seguire questi passaggi:

1. Selezionare il tasto stato del backup.
2. Cliccare sul tasto **Risolvere** per risolverli uno alla volta oppure il tasto**Risolvere tutti adesso** per risolverli tutti inmediatamente.
3. Se un problema non venisse risolto subito, seguire i passaggi dell'assistente per risolverlo.

Nota
Per ulteriori informazioni su queste procedure, vi preghiamo di riferirvi alla sezione «*Backup*» (p. 28).

3.4. Tasto Stato del TuneUp

Se il tasto di stato del tuneup è verde, non c'è niente di cui preoccuparsi. Altrimenti, se il tasto è giallo o rosso, il vostro computer è esposto ad un rischio di sicurezza medio o alto.

Il colore dei tasti di stato può cambiare, non solo quando configurate le impostazioni che potrebbero colpire la sicurezza del vostro computer, ma anche quando dimenticate di eseguire funzioni importanti.

Per esempio, se non avete eseguito una deframmentazione del vostro computer da molto tempo, il tasto di stato sarà rosso.

La tabella sotto vi fornirà l'informazione su gli elementi tenuti in conto per il calcolo del rischio di sicurezza.

Problema	*Colore*
L'ultima pulizia dei file di Internet e cookies è vecchia	Giallo
L'ultima pulizia dei file di Internet e cookies è molto vecchia	Rosso
L'ultima pulizia del registro è vecchia	Giallo
L'ultima pulizia del registro è molto vecchia	Rosso
L'ultima pulizia dei file duplicati è vecchia	Giallo
L'ultima deframmentazione è vecchia	Giallo
L'ultima deframmentazione è molto vecchia	Rosso

Per risolvere i problemi, vi invitiamo a seguire questi passaggi:

1. Selezionare il tasto di stato del tuneup.
2. Cliccare sul tasto **Risolvere** per risolverli uno alla volta oppure il tasto**Risolvere tutti adesso** per risolverli tutti inmediatamente.
3. Se un problema non venisse risolto subito, seguire i passaggi dell'assistente per risolverlo.

Nota
Per ulteriori informazioni su queste procedure, vi preghiamo di riferirvi alla sezione «*TuneUp*» (p. 37).

4. Funzioni Veloci

Sotto i quattro tasti di stato vengono mostrate tre sezioni, corrispondenti ai tre tipi di funzioni di sicurezza:

- **Sicurezza**
- **Backup**
- **TuneUp**

4.1. Sicurezza

BitDefender contiene un modulo di Sicurezza che vi aiuta a mantenere il vostro BitDefender aggiornato ed il vostro computer libero di virus.

Per accedere al modulo Sicurezza, cliccare sulla linguetta **Sicurezza**.

Sono disponibili i seguenti tasti:

- **Aggiornare adesso** - inizia un aggiornamento silenzioso.
- **Esamina Documenti** - inizia una scansione veloce dei vostri documents and settings.
- **Scansione Completa del Sistema** - inizia una scansione completa del vostro computer.

4.1.1. Aggiornamento

Il processo di aggiornamento viene eseguito involo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodottoe, nello stesso tempo, ogni vulnerabilità verrà esclusa.

4.1.2. Scanner di BitDefender.

Quando si inizializza un processo di scansione a richiesta, sia scansione veloce o completa, lo Scanner di BitDefender apparirà.

Seguire la procedura di tre passi per completare il processo di scansione.

Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.

Scansione

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Nota
La durata del processo dipende dalla complessità della scansione.

Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

Potete fermare la scansione in qualsiasi momento, cliccando su**Fermare**. Verrete portati all'ultimo passo dell'assistente.

Nota
Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di sottoporli al Lab BitDefender.

Attendere che BitDefender finisca la scancione.

Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.

Le seguenti opzioni possono comparire nel menu:

Azione	*Descrizione*
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati.

Azione	Descrizione
Disinfettare	Disinfetta i file infetti.
Eliminare	Elimina i file infetti.
Mostrare	Rende visibili i file nascosti

Click **Risolvere i problemi** per applicare le azioni specificate.

Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.

Sommario

E' possibile visualizzare il sommario dei risultati.

Il file di report viene automaticamente salvato nella sezione Registri della finestra delle **Proprietà** di ogni funzione.

Avvertimento
Se ci sono problemi non risolti, vi consigliamo di contattare il Team di suppoto di BitDefender su www.bitdefender.com.

4.2. Backup

BitDefender arriva con un modulo di backup che vi aiuta a fare copie di riserva di ogni prezioso dato sul vostro sistema. Potete eseguire il backup dei dati sul vostro computer, su dischi rimuovibili o su di una ubicazione di rete per essere sicuri di poter recuperarli quando sia necessario. Il recupero dei vostri dati è un processo facile.

Per accedere al modulo Backup cliccare sulla sezione **Backup** sotto i quattro tasti di stato.

Sono disponibili i seguenti tasti:

- **Iniziare l'Assistente di Backup** - avvia una facile procedura di cinque passi per eseguire il backup dei vostri dati.
- **Impostazioni Avanzate** - qui potete impostare ed eseguire operazioni di backup in dettaglio.
- **Iniziare l'Assistente di Recupero** - avvia una facile procedura di quattro passi per eseguire il recupero dei vostri dati.

4.2.1. Avviare Assistente di Backup

Cliccando **Avviare Assistente di Backup** un assistente vi guiderà attraverso il processo di creazione di una funzione di backup. Alla fine di questo processo sarete in grado di eseguire subito il backup dei vostri dati, o di programmare il prodotto per eseguire il backup in un secondo momento.

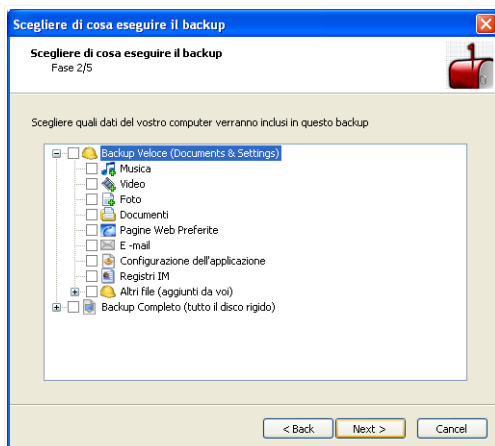
Passo 1/5 - Finestra di Benvenuto

Questa è solo una pagina di benvenuto.

Finestra di benvenuto

Selezionare **Avanti**.

Passo 2/5 - Scegliere su cosa eseguire il backup

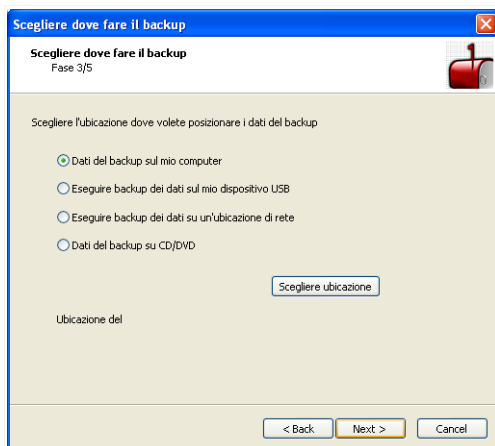
Qui potete selezionare i dati del vostro computer su cui eseguire il backup.

Scegliere su cosa eseguire il backup

Potete scegliere tra **Backup Veloce** (musica, video, foto, email, impostazioni di applicazioni, etc.) o **Backup Completo** (tutte le partizioni).

Cliccare **Altri file**, per aggiungere altri file dal vostro desktop al **Backup Veloce**. Il **Backup Completo** può essere anche facilmente personalizzato selezionando le directory di una certa partizione sulle quali eseguire il backup.

Selezionare **Avanti**.

Passaggio 3/5 - Scegliere dove eseguire il backup

Qua potete selezionare l'ubicazione dei dati sui quali è stato eseguito il backup.

Scegliere dove eseguire il backup

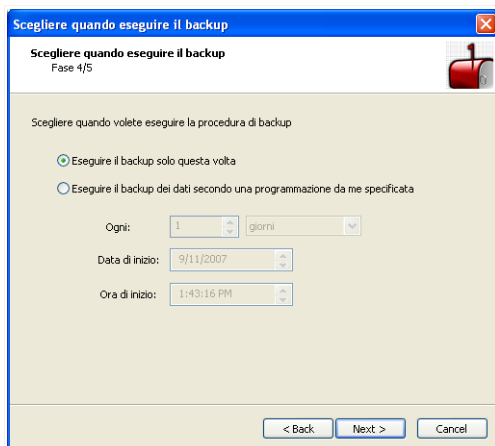
Sono disponibili le seguenti opzioni:

- **Eseguire il Backup dei dati sul mio computer**
- **Eseguire il Backup dei dati sul mio dispositivo USB**
- **Eseguire il Backup dei dati su un'ubicazione di rete**
- **Eseguire il Backup dei dati su CD/DVD**

Se decidete di esguire il backup dei vostri dati sul vostro computer, dispositivo USB o un'ubicazione di rete, cliccare su **Scegliere ubicazione** e selezionare dove salvare i dati.

Selezionare **Avanti**.

Passo 4/5 - Scegliere quando eseguire il Backup

Qua potete scegliere quando eseguire il backup dei vostri dati.

Scegliere quando eseguire il Backup

Sono disponibili le seguenti opzioni:

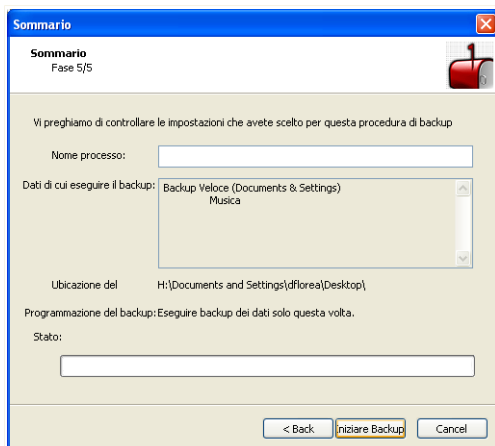
- **Eseguire il backup dei dati solo questa volta**
- **Eseguire il backup dei dati con una programmazione da me specificata**

Per eseguire subito il backup dei dati, cliccare su **Eseguire il backup dei dati solo questa volta**, per programmare il prodotto in modo da eseguire il backup dei vostri file in un secondo momento, cliccare su **Eseguire il backup dei dati con una programmazione da me specificata**.

Se selezionate **Eseguire il backup dei dati con una programmazione da me specificata**, potrete specificare la frequenza con cui la funzione programmata verrà eseguita: giornalmente o settimanalmente. Potrete anche specificare la data e l'ora di inizio.

Selezionare **Avanti**.

Passo 5/5 - Sommario

Qui potete rivedere le impostazioni del lavoro di backup.

Sommario

Dovete inserire un nome della funzione nel campo corrispondente.

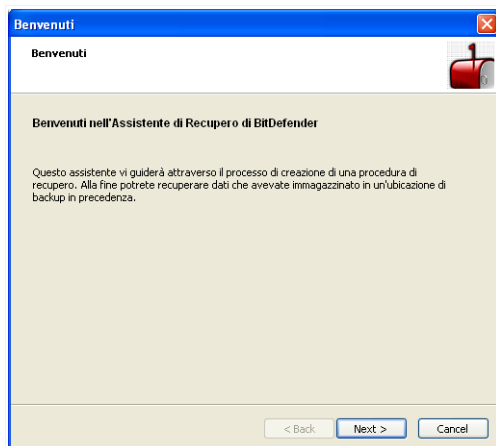
Cliccare su **Avviare backup** se siete soddisfatti delle vostre impostazioni.

Selezionare **Termina**.

4.2.2. Avviare Assistente di Recupero

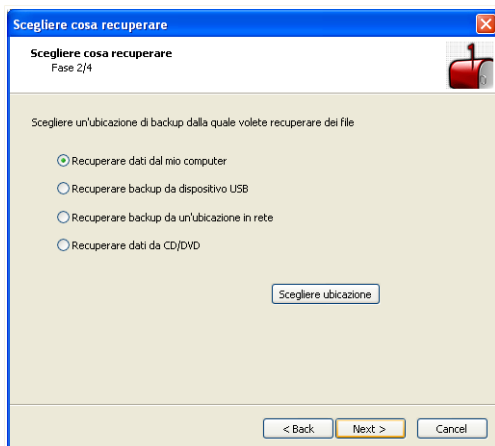
Cliccando su **Avviare Assistente di Recupero** un assistente vi guiderà attraverso il processo di recupero dei vostri dati su cui avete eseguito il backup.

Passo 1/4 - Finestra di Benvenuto

Questa è solo una pagina di benvenuto.

Finestra di benvenuto

Selezionare **Avanti**.

Passo 1/4 -Scegliere da dove eseguire il Recupero.

Qui potete scegliere l'ubicazione da dove volete recuperare i file.

Scegliere da dove eseguire il Recupero

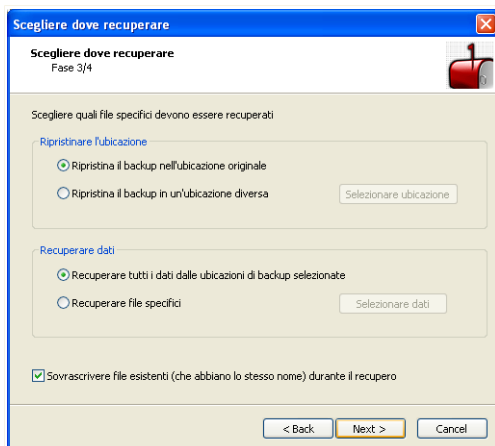
Sono disponibili le seguenti opzioni:

- **Recuperare i dati dal mio computer**
- **Recuperare backup da un dispositivo USB**
- **Recuperare backup da un'ubicazione di rete**
- **Recuperare backup da un CD/DVD**

Selezionare **Scegliere ubicazione** e selezionare da dove salvare i dati.

Selezionare **Avanti**.

Passo 3/4 - Scegliere Ubicazione di Recupero e File

Qui potete scegliere quali specifici file recuperare e dove ripristinarli.

Scegliere l'ubicazione di recupero e i file

Sono disponibili le seguenti opzioni:

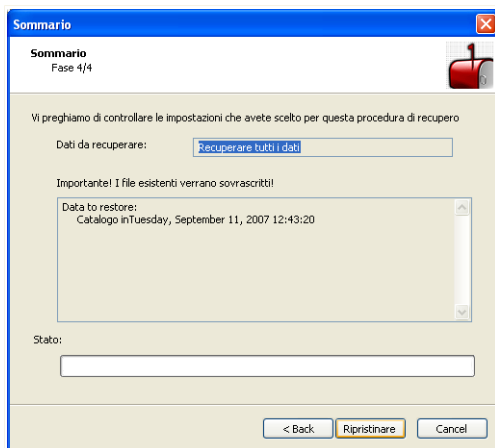
- **Ripristinare il backup nell'ubicazione originale**
- **Ripristinare il backup in un'ubicazione diversa**
- **Ripristinare tutti i dati dall'ubicazione di backup selezionata**
- **Ripristinare file specifici**
- **Sostituire file esistenti durante il ripristino**

Se volete ripristinare dei dati in un'ubicazione diversa o solo file specifici, selezionare l'ubicazione e i dati cliccando sul tasto corrispondente.

Per evitare di sostituire file esistenti durante il ripristino, deselezionare il corrispondente tasto radio.

Selezionare **Avanti**.

Passo 4/4 - Sommario

Qui potete rivedere le impostazioni del lavoro di recupero.

Cliccare su **Ripristinare** se siete soddisfatti con le vostre impostazioni.

Selezionare **Termina**.

4.3. TuneUp

BitDefender arriva con un modulo Tuneup che vi aiuta a mantenere l'integrità del vostro sistema. Gli strumrnti di manutenzione offerti sono critici per il miglioramenti della reattività del vostro sistema e la gestione efficace dello spazio sul disco rigido.

Per eseguire operazioni di manutenzione sul vostro PC, cliccare sulla sezione **TuneUp** ed utilizzare gli strumenti forniti. Sono disponibili i seguenti tasti:

- **Deframmentazione Dischi** - Inizia la procedura che vi permette di deframmentare i dischi locali.
- **Trovare File Duplicati** - Inizia la procedura che vi permette di trovare ed eliminare file duplicati.
- **Cancella File Internet** - Inizia la procedura che vi permette di cancellare file temporanei Internet e cookies.
- **Cancellare file definitivamente** - Inizia la procedura che vi permette di rimuovere file dal vostro computer definitivamente, in modo permanente.
- **Pulire Registro** - Inizia la procedura che vi permette di pulire il Registro di Windows.
- **Recuperare Registro** - Inizia la procedura che vi permette di recuperare il Registro di Windows pulito.

4.3.1. Deframmentazione dei Volumi del Disco Rigido.

Quando si copia un file che eccede il blocco più grande di spazio libero su disco rigido, si verifica una frammentazione del file. Siccome non c'è spazio libero sufficiente per immagazzinare l'intero file in modo continuo, verrà immagazzinato in diversi blocchi. Quando si accede al file frammentato, i suoi dati devono essere letti da diverse ubicazioni.

La frammentazione del file rallenta l'accesso allo stesso e diminuisce le prestazioni del sistema. Questo accellera anche l'usura del disco rigido.

Per ridurre la frammentazione dei file dovete deframmentare i dischi periodicamente. La deframmentazione fisica dei dischi riorganizza i dati sul disco rigido in modo che i pezzi di ogni file vengano immagazzinati assieme ed in modo continuo. Questo tenta anche di creare aree di spazio libero più grandi per evitare che i file vengano frammentati dopo.

Si consiglia di deframmentare il disco rigido per:

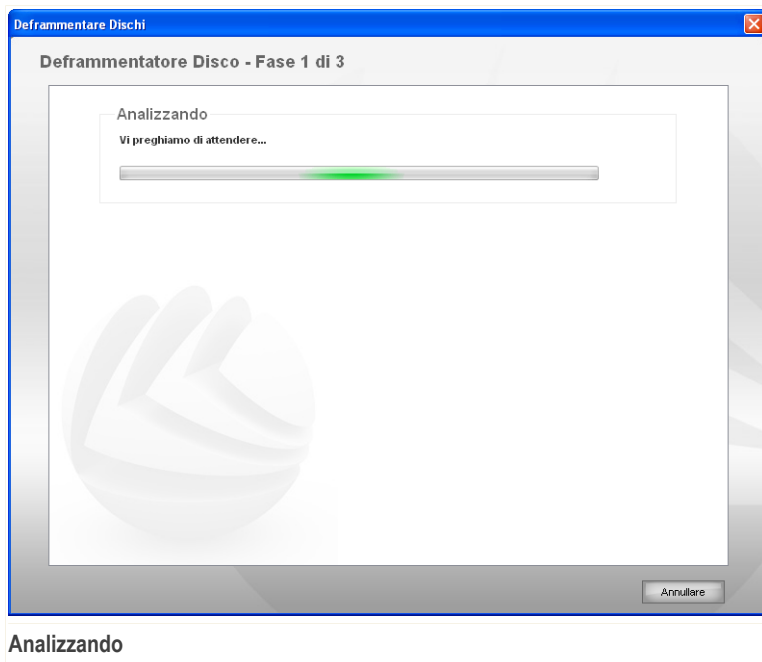
- accedere più velocemente ai file.
- migliorare le prestazioni del sistema in generale.
- prolungare la vita del disco rigido.

Per deframmentare il disco rigido, cliccare sulla sezione **TuneUp** del Centro di Sicureza e quindi **Deframmentare dischi**. Dovrete completare una procedura guidata di tre passi.

Nota

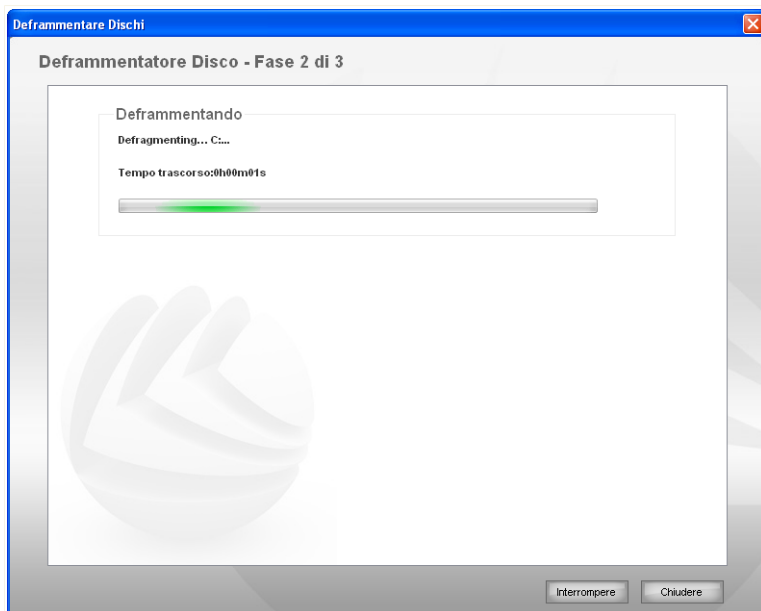
La deframmentazione può impiegare un po' di tempo dal momento in cui implica lo spostamento di porzioni di dati immagazzinati da un posto all'altro del disco rigido. Vi consigliamo di eseguire la deframmentazione quando non state usando il vostro computer.

Passo 1/3 - Analisi...

Il Deframmentatore analizzerà il disco rigido per determinare se necessita di essere deframmentato o meno.

Analizzando

Attendere che il Deframmentatore finisca l'analisi.

Passo 2/3 - Visualizzare Report di Analisi

Dopo che l'analisi è stata completata, apparirà una nuova finestra dove potrete vedere i risultati ed iniziare la deframmentazione del disco, se necessaria.

Report di Analisi

Controllare il report di analisi. Se c'è un disco che necessita la deframmentazione, selezionare **Eseguire** per deframmentarlo.

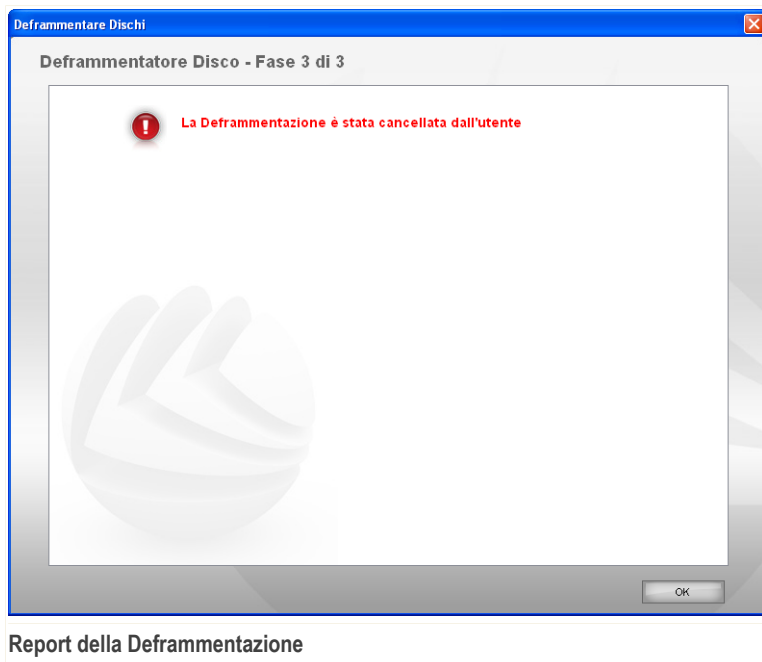
La deframmentazione del disco avrà inizio. Potete cancellarla in qualsiasi momento cliccando su **Interrompere**.

Nota
Il Deframmentatore avrà bisogno del 15% di spazio libero nel volume deframmentato per operare correttamente. Se nonc'è spazio libero sufficiente nel volume deframmentato, la deframmentazione verrà interrotta.

Attendere il completamento della deframmentazione del disco.

Passo 3/3 - Visualizzare Report della Deframmentazione

Dopo che la deframmentazione del disco è stata completata, apparirà una nuova finestra dove potrete vedere le statistiche della deframmentazione.

Report della Deframmentazione

Selezionare **OK** per chiudere la finestra.

4.3.2. Trovare file duplicati

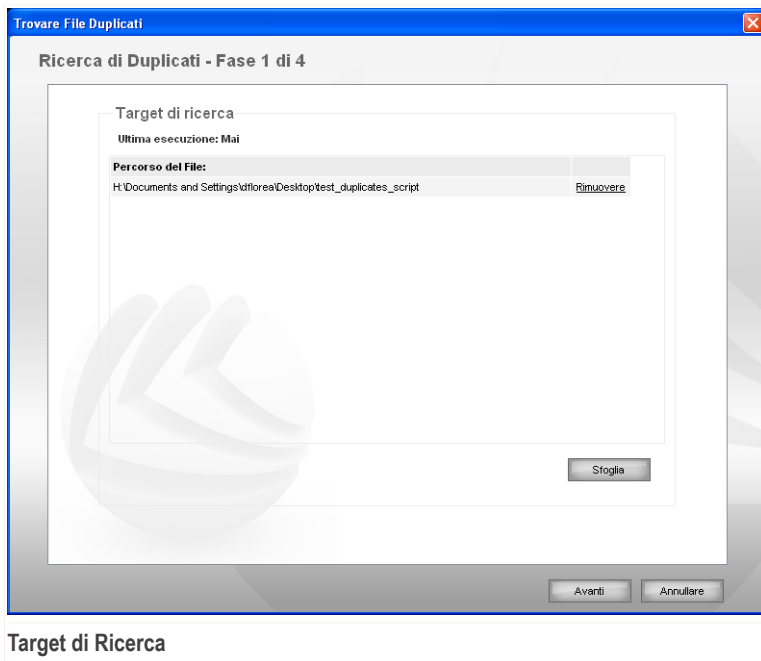
I file duplicati si mangiano lo spazio del vostro disco rigido. Pensate solo di avere lo stesso file `.mp3` salvato in tre ubicazioni diverse.

Per rilevare ed eliminare file duplicati dal vostro computer, potete utilizzare il Duplicate Finder. In questo modo potrete migliorare la gestione dello spazio libero sui vostri dischi rigidi.

Per trovare dei duplicati, cliccare sulla sezione **TuneUp** nel Centro di Sicurezza e quindi **Trovare File Duplicati**. Dovrete completare una procedura guidata di quattro passi.

Passo 1/4 – Selezione del Target di ricerca

Qui potete specificare dove cercare i duplicati.

Target di Ricerca

Cliccare su **Sfoglia** e selezionare l'ubicazione dove il Duplicate Finder deve cercare i file duplicati.

Nota

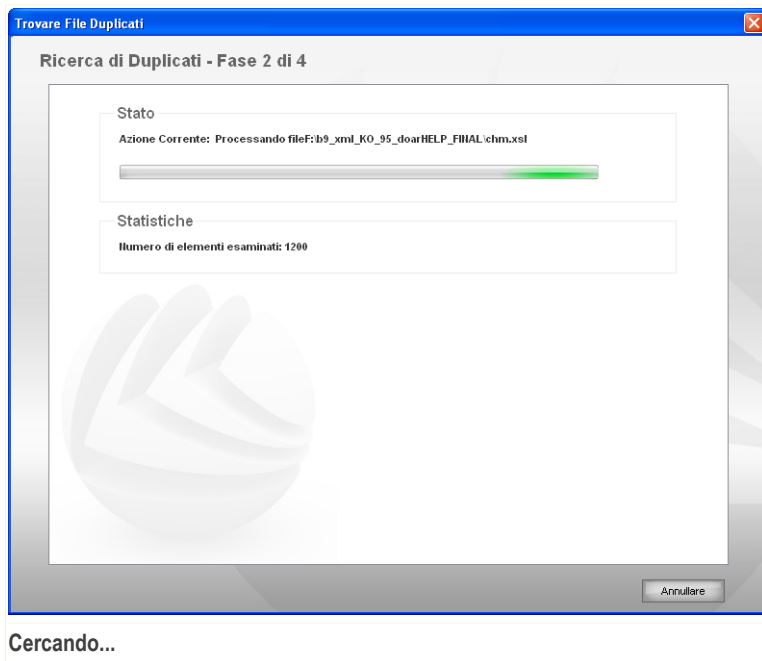
E' possibile selezionare una o più ubicazioni.

Il percorso dell'ubicazione selezionata apparirà nella colonna **Percorso File**. Se campiate idea riguardo l'ubicazione, cliccare semplicemente sul tasto **Rimuovere**.

Selezionare **Avanti**.

Passo 2/4 – Ricerca...

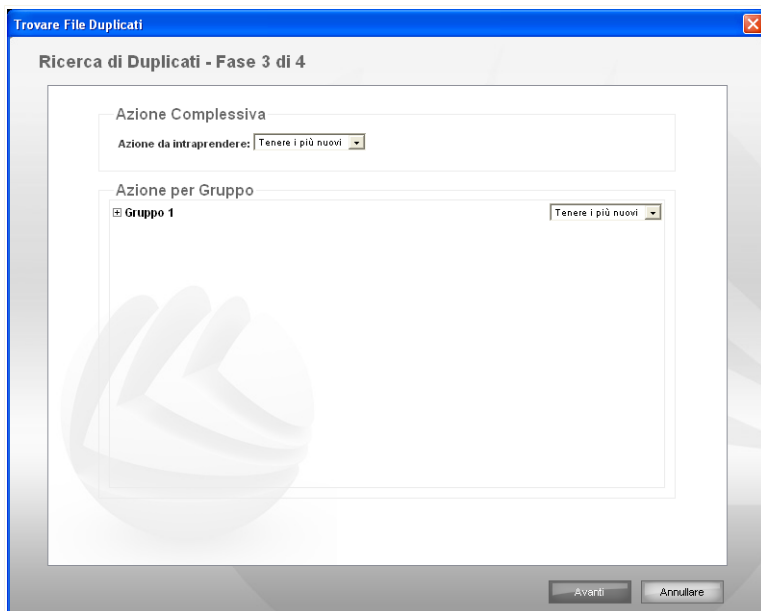
Il Duplicate Finder inizierà a cercare i file duplicati.

Cercando...

Potete veder lo stato e le statistiche della ricerca.

Attender che il Duplicate Finder finisca la ricerca di file duplicati.

Passo 3/4 – Selezionare azione

Dopo che la ricerca è stata completata, apparirà una nuova finestra dove potrete specificare quali azioni intraprendere sui file duplicati rilevati.

Nota
Se nessun file duplicato è stato trovato, ignorerete questo passo.

Azioni

Potete scegliere un'azione complessiva da eseguire su tutti i file duplicati rilevati oppure potete scegliere delle azioni da eseguire su gruppi di file duplicati.

Sono disponibili le seguenti opzioni:

Azione	Descrizione
Mantenere il più recente	Il duplicato più recente verrà conservato, mentre gli altri verranno eliminati.
Mantenere il più vecchio	Il duplicato più vecchio verrà conservato, mentre gli altri verranno eliminati.
Nessuna azione	Nessuna azione verrà eseguita sui file duplicati.

Cliccare sul "+" accanto ad un gruppo per vedere gli oggetti che contiene. Se volete applicare un'azione complessiva a tutti gli oggetti di un gruppo, selezionare l'azione

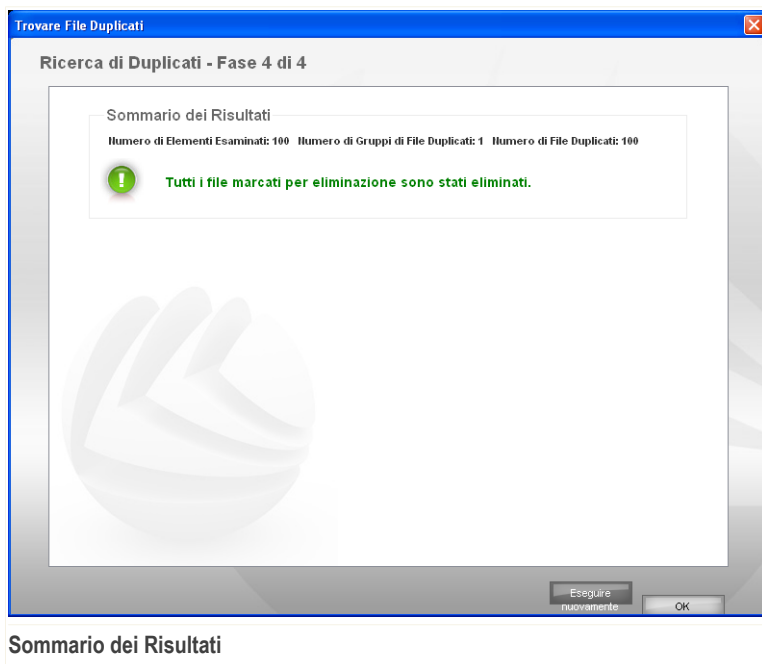
desiderata dal menu corrispondente. Se volete che vengano leiminati solo dei file specifici del gruppo, selezionate l'opzione **Eliminare** accanto ai rispettivi file.

Nota
L'azione complessiva non sovrascriverà l'azione scelta per file specifici o gruppi. Questo significa che, se impostate, per esempio, **Mantenere il più recente** come azione complessiva ma scegliete di non eseguire alcuna azione su di un gruppo in particolare, allora l'azione complessiva verrà applicata a tutti, tranne che a quel gruppo particolare.

Selezionare **Avanti**.

Passo 4/4 - Visualizzare Sommario dei Risultati

Qui potete visualizzare i risultati della scansione del Duplicate Finder.

Sommario dei Risultati

Selezionare **OK** per chiudere la finestra.

4.3.3. Pulizia dei File Internet

Ogni volta che visitate una pagina web, vengono creati dei file temporanei Internet per permettervi un accesso più veloce la volta successiva.

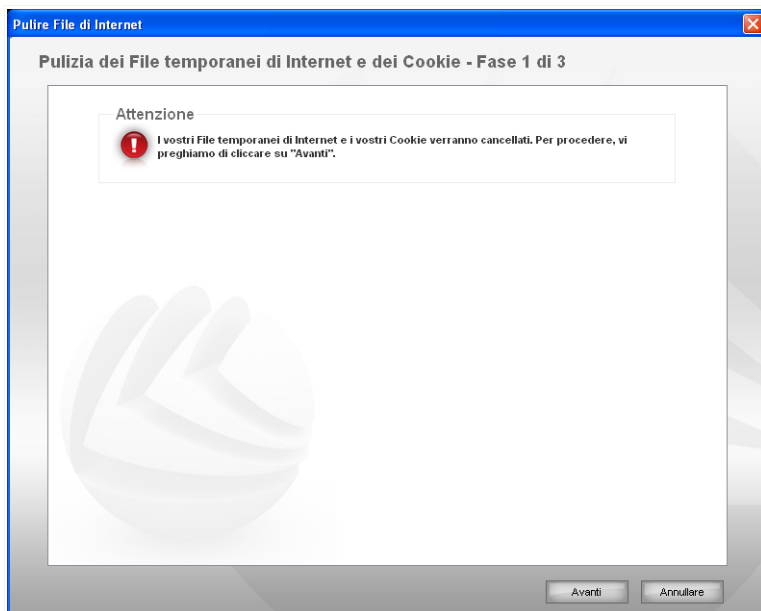
Nonostante vengono riferiti come temporanei, questi file non vengono eliminati quando chiudete il browser. Questo può diventare un problema di privacy poichè questi file possono essere visti da chiunque abbia accesso al vostro computer. Inoltre, con il tempo, questi file raggiungono una dimensione considerevole, mangiandosi lo spazio del vostro disco rigido.

Anche i cookies vengono immagazzinati nel vostro computer quando visitate una pagina web. I cookies son dei piccoli file contenenti informazioni sulle vostre preferenze di navigazione. Essi potrebbero essere visti anche come un problema di privacy, poichè possono essere analizzati ed usati dai pubblicisti per tarcciare i vostri interessi e gusti on line.

Pulendo i file temporanei Internet ed i cookies libererete spazio sul disco e proteggerete la vostra privacy.

Per pulire la cartella dei file temporanei Internet, dove Internet Explorer salva i suoi file temporanei Internet e cookies, cliccare nella sezione **TuneUp** del Centro di Sicurezza e quindi **Pulire i File Internet**. Dovrete completare una procedura guidata di tre passi.

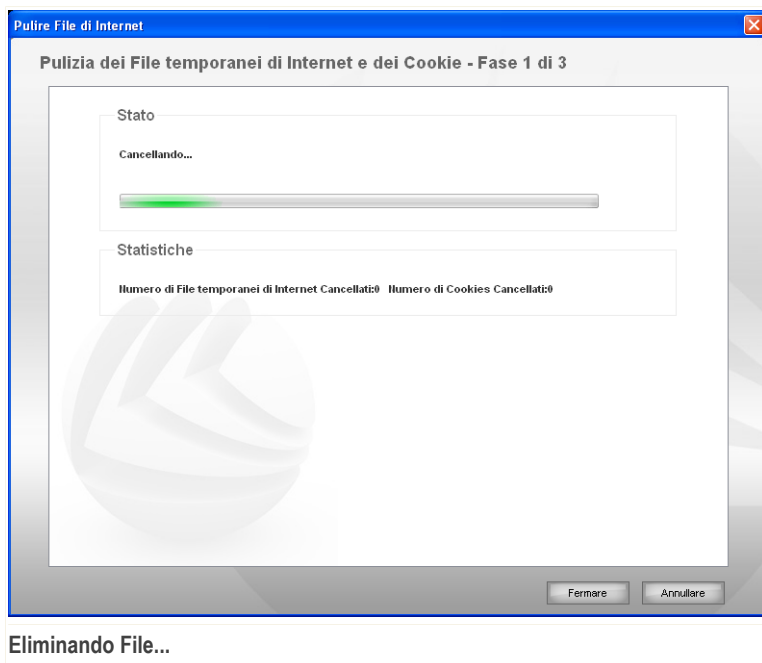
Passo 1/3 – Iniziare Eliminazione

Qua potete inziziare ad eliminare i file temporanei Internet ed i cookies.

Finestra di benvenuto

Selezionare **Avanti**.

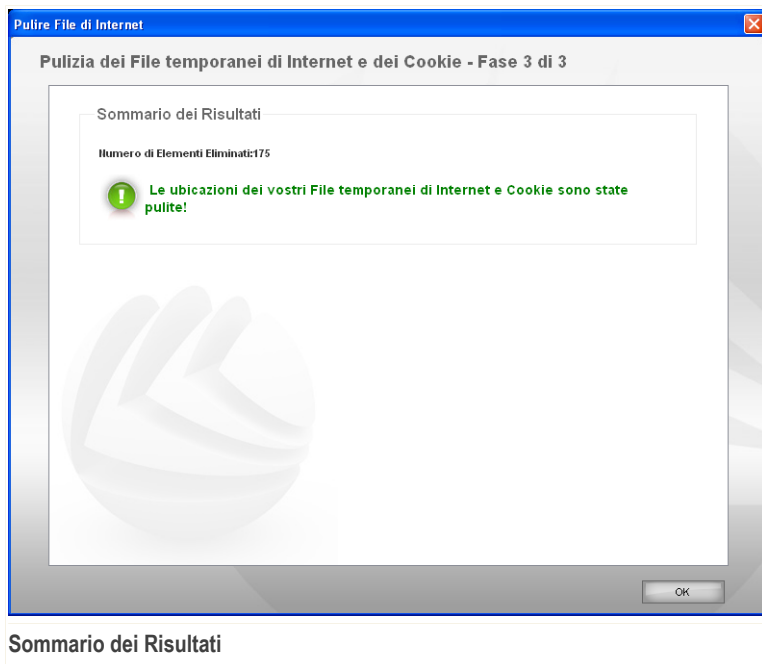
Passo 1/3 – Eliminando file...

Lo strumento di pulizia inizierà ad eliminare i file temporanei Internet ed i cookies.

Eliminando File...

Attendere che lo strumento di pulizia elimini i file temporanei Internet ed i cookies.

Passo 3/3 - Visualizzare Sommario dei Risultati

Dopo che lo strumento di pulizia ha eliminato tutti i file, apparirà una nuova finestra nella quale potrete vedere il sommario dei risultati.

Sommario dei Risultati

Potete vedere le statistiche riguardanti gli oggetti eliminati.

Selezionare **OK** per chiudere la finestra.

4.3.4. Eliminazione Definitiva dei File

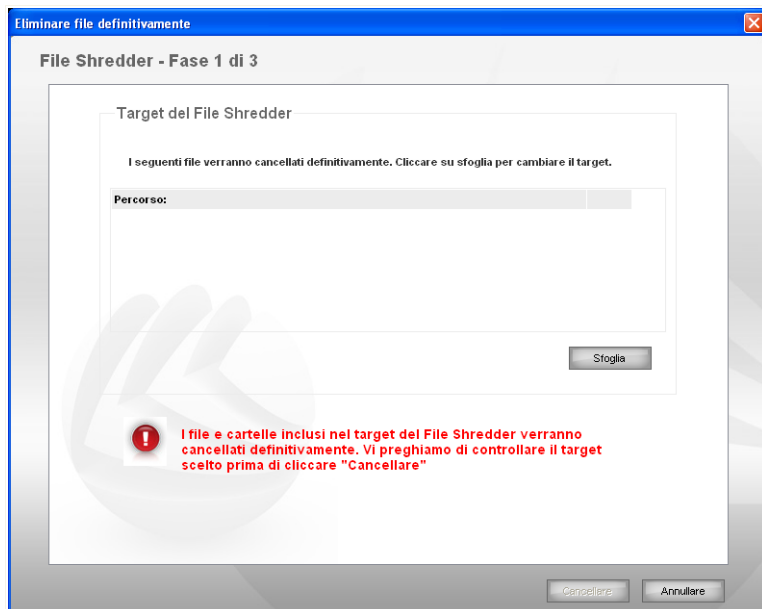
Quando eliminate un file, non si può più accedere ad esso con i normali strumenti. Comunque, il file continua ad essere immagazzinato sul disco rigido finchè non verrà sovrascritto quando copierete nuovi file.

Anche se eliminate un file, esso può essere recuperato utilizzando dei programmi specializzati. Questo potrebbe rappresentare una minaccia alla vostra privacy, poichè ci potrebbero essere dei tentativi maligni di prendere i vostri dati privati.

Per evitare che i dati sensibili vengano recuperati dopo che li avete eliminati, potete utilizzare BitDefender per eliminarli definitivamente, rimuovendoli fisicamente dal vostro disco rigido.

Per rimuovere definitivamente i file, cliccare sulla sezione **TuneUp** nel Centro di Sicurezza e quindi **Eliminare File Definitivamente**. Dovrete completare una procedura guidata di tre passi.

Passo 1/3 - Selezionare Target

Qua potete specificare i file o cartelle da rimuovere definitivamente.

Target

Cliccare **Sfoglia**, selezionare i file o cartelle che volete eliminare e cliccare **OK**.

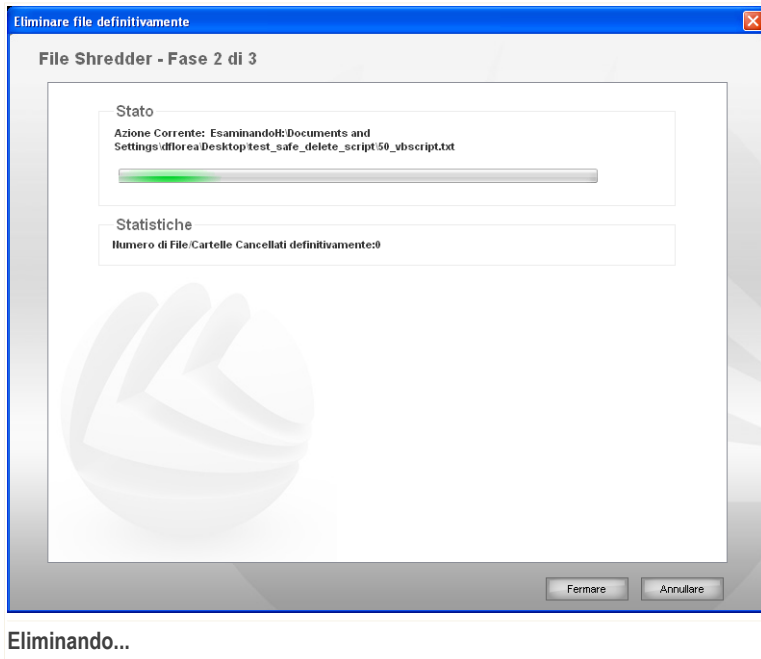
Nota
E' possibile selezionare una o più ubicazioni.

Il percorso dell'ubicazione selezionata apparirà nella tabella. Se cambiate idea sull'ubicazione, selezionarla e cliccare **Rimuovere**.

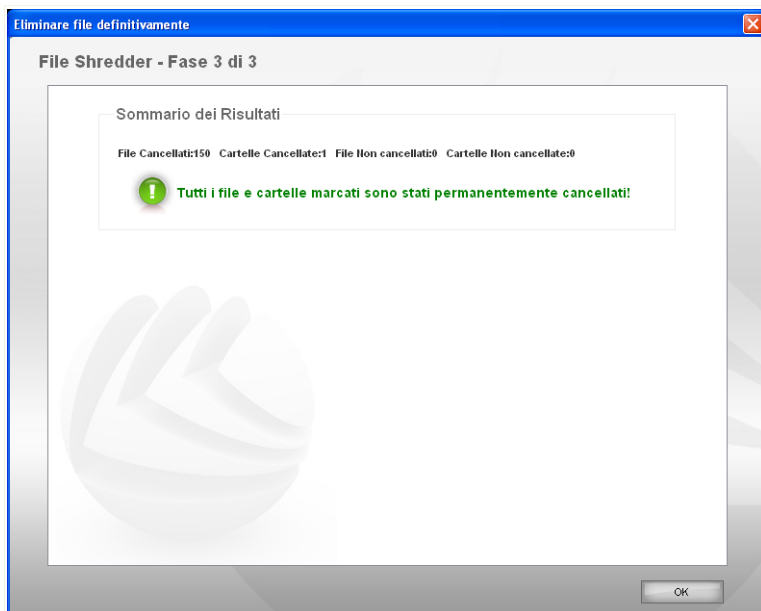
Cliccare **Eliminare**.

Passo 1/3 – Eliminando file...

BitDefender eliminerà definitivamente i file nelle ubicazioni specificate.

Eliminando...

Attendere il completamento di questa operazione.

Passo 3/3 - Visualizzare Sommario dei Risultati

Dopo che tutti i file saranno stati rimossi, apparirà una nuova finestra dove potrete visualizzare i risultati.

Sommario dei Risultati

Selezionare **OK** per chiudere la finestra.

4.3.5. Pulizia del Registro

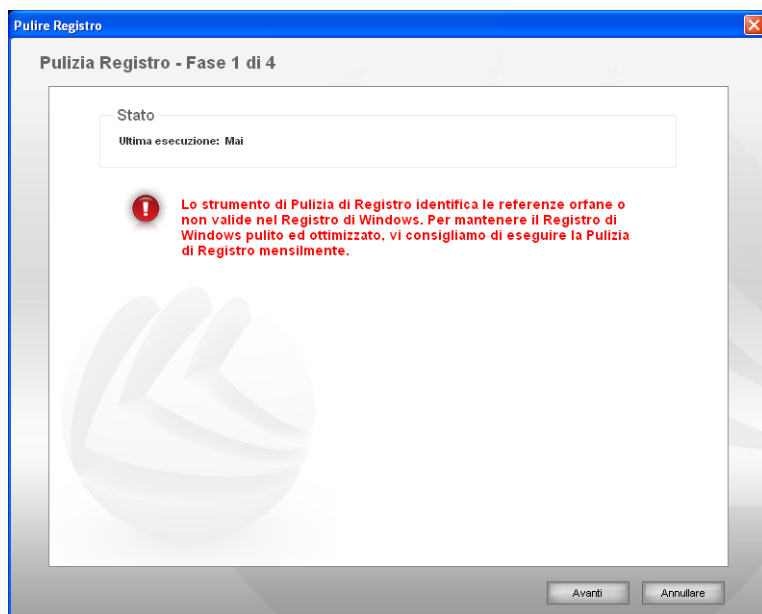
Il Registro di Windows è una parte importante dei sistemi operativi Windows. Esso è un database che contiene informazioni ed impostazioni per l'hardware ed il sistema operativo, applicazioni installate, utenti, preferenze del vostro computer ed altro.

Molte applicazioni scrivono delle chiavi nel Registro di Windows al momento dell'installazione. Quando tali applicazioni vengono rimosse, alcune delle chiavi di registro associate potrebbero non venire eliminate e rimanere nel Registro di Windows, rallentando il vostro sistema e causando addirittura instabilità nel sistema. La stessa cosa accade quando eliminate dei collegamenti o certi file di applicazioni installate nel vostro sistema, così come nel caso di driver corrotti.

Per pulire il Registro di Windows e migliorare le prestazioni del vostro sistema, utilizzare lo Strumento di Pulizia del Registro. Lo Strumento di Pulizia esamina il Registro di Windows ed elimina le chiavi di registro non valide.

Per pulire il Registro di Windows, cliccare nella sezione **TuneUp** del Centro di Sicurezza e quindi **Pulire Registro**. Dovrete completare una procedura guidate di quattro passi.

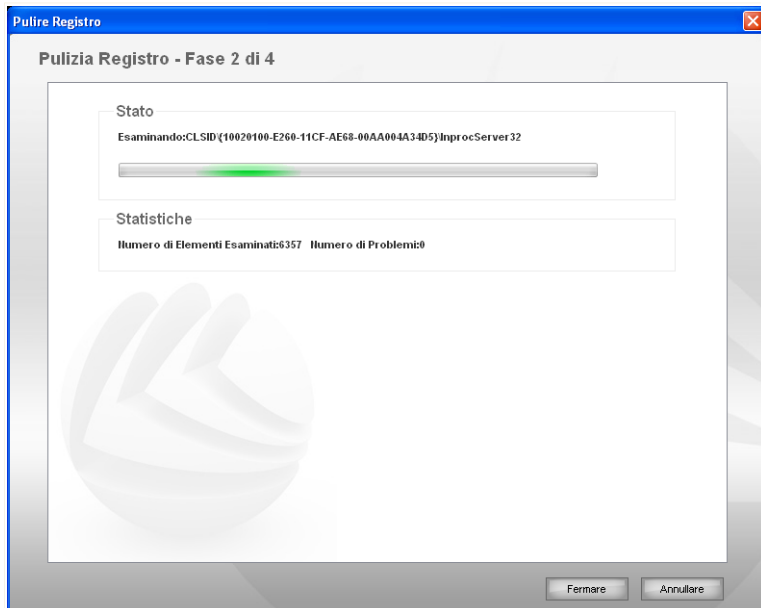
Passo 1/4 - Iniziare scansione

Qua potete avviare la scansione del registro.

Stato

Potete vedere quando è stata eseguita per l'ultima volta la Pulizia del Registro e la raccomandazione di BitDefender.

Selezionare **Avanti**.

Passo 2/4 - Esaminando...

Lo Strumento di Pulizia di Registro avvierà la scansione del Registro di Windows.

Esaminando...

Potete vedere l'ultima chiave di registro esaminata e le relative statistiche.

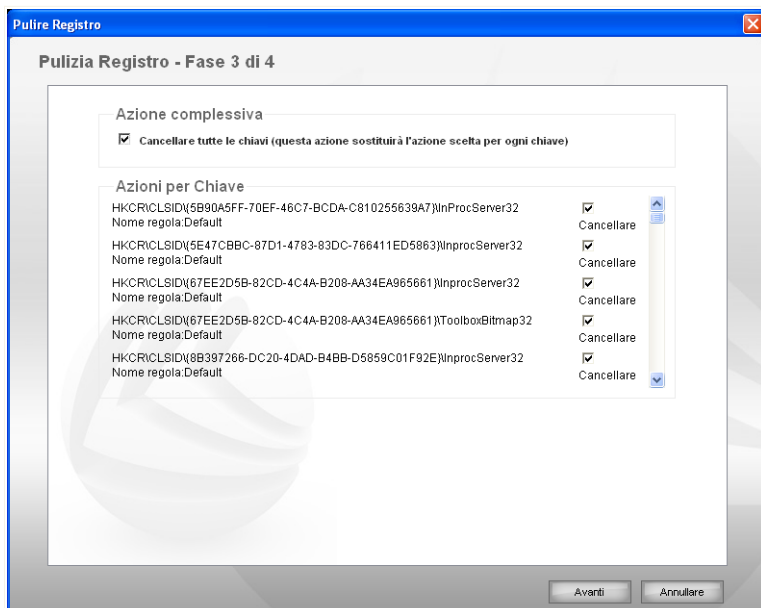
Attendere che lo Strumento di Pulizia di Registro completi la scansione della chiave di registro.

Nota
Se volete fermare la scansione, cliccate semplicemente **Fermare**. Ignorerete il passo seguente.

Passo 3/4 – Selezionare azione

Una volta completata la scansione delle chiavi di registro, apparirà una nuova finestra dove potrete vedere i risultati.

Nota

Se non viene riscontrato alcun problema o se avete scelto di fermare la scansione, ignorerete questo passo.

Azioni

Potete vedere tutte le chiavi di registro rilevate. Potete scegliere di eliminarle tutte oppure solo quelle specificate.

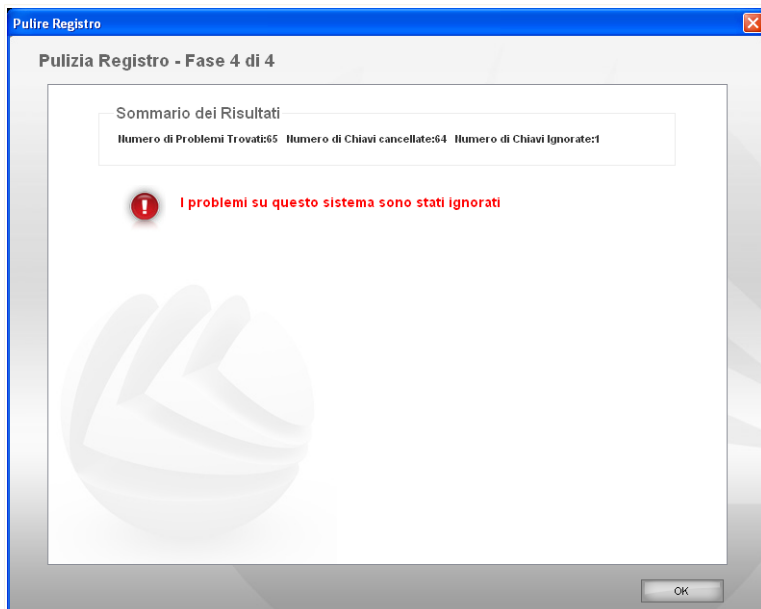
Se selezionate **Eliminare tutte le chiavi** tutte le chiavi rilevate verranno eliminate. Se desiderate eliminare solo delle chiavi specifiche, selezionate l'opzione **Eliminare** accanto alle rispettive chiavi.

Nota

Di default, tutte le chiavi non valide rilevate verranno eliminate.

Selezionare **Avanti**.

Passo 4/4 - Visualizzare Sommario dei Risultati

Qui potete vedere i risultati della scansione eseguita dallo Strumento di Pulizia di Registro.

Sommario dei Risultati

Se non avete scelto di eliminare tutte le chiavi di registro, vi verrà mostrato un testo di avviso. Vi consigliamo di rivedere i rispettivi problemi.

Selezionare **OK** per chiudere la finestra.

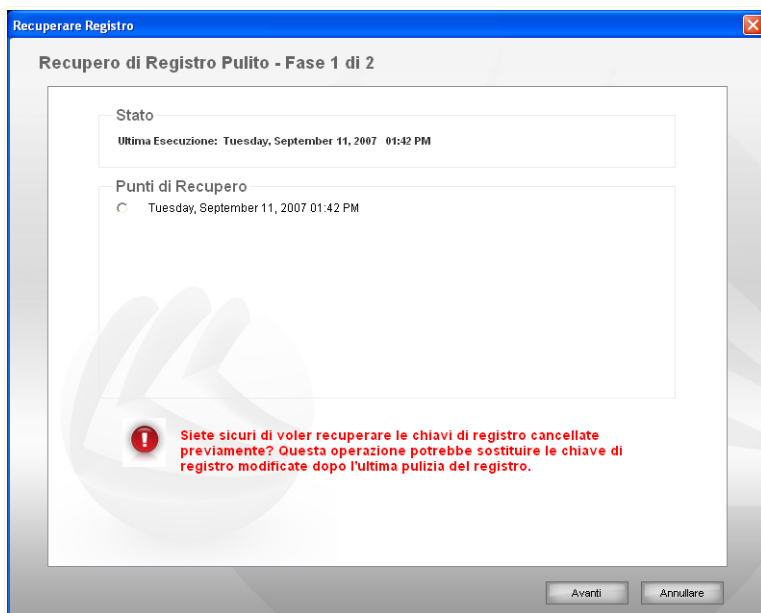
4.3.6. Recupero di Registro Cancellato

A volte, dopo la pulizia del registro, potreste notare che il vostro sistema non lavora bene, o che alcune applicazioni non operano correttamente, a causa di chiavi di registro mancanti. Questo può essere causato da chiavi di registro condivise che sono state eliminate durante la pulizia del registro o da altre chiavi eliminate. Per risolvere questo problema dovete recuperare il registro pulito.

Per recuperare il registro pulito, cliccare nella sezione **TuneUp** del Centro di Sicurezza e quindi **Recuperare Registro**. Dovrete completare una procedura guidata di due passi.

Importante
Solo gli utenti con diritti di amministrazione possono recuperare il registro pulito.

Passo 1/2 - Avviare Recupero del Registro

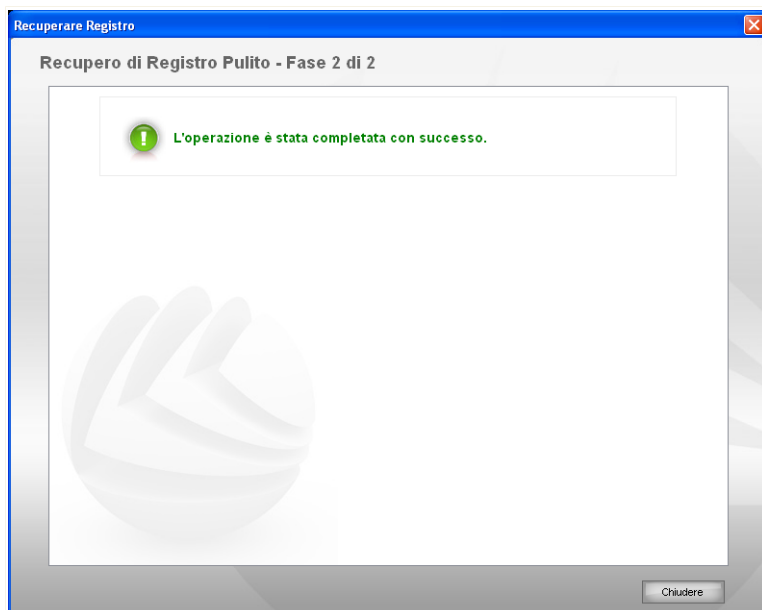
Qui potete avviare il recupero del registro pulito.

Stato

Potete vedere quando è stato pulito l'ultima volta il Registro di Windows.

Se siete sicuri di voler recuperare il registro pulito, cliccare **Avanti**.

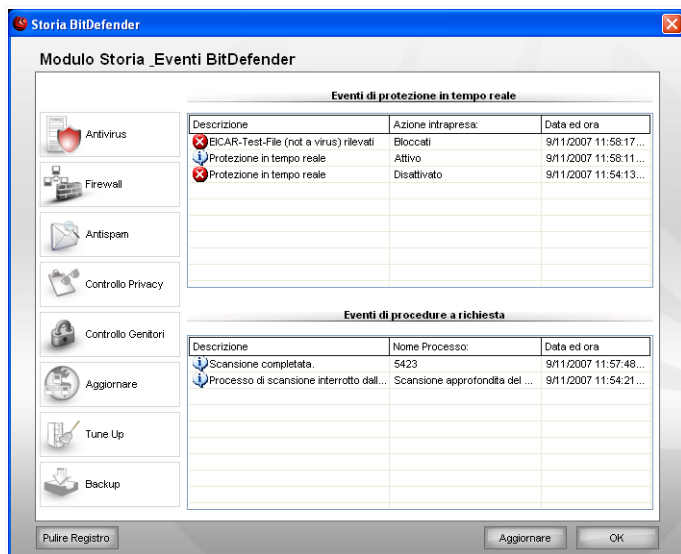
Avvertimento
Il recupero del registro pulito potrebbe sovrascrivere le chiavi di registro modificate dopo l'ultima pulizia.

Passo 2/2 - Visualizzare Risultati

Qui potete vedere se il recupero è stao eseguito con successo.

Risultati

Selezionare **OK** per chiudere la finestra.

5. Storia

Il link **Storia**, in fondo alla finestra del Centro di Sicurezza BitDefender, apre un'altra finestra con la storia ed eventi di BitDefender. Questa finestra vi offre una visione generale degli eventi relativi alla sicurezza. Per esempio, potete potete controllare facilmente se l'aggiornamento è stato eseguito con successo, se è stato rilevato del malware sul vostro computer, se i vostri processi di backup si eseguono senza errore, etc.

Eventi

Per aiutarvi a filtrare la storia ed eventi di BitDefender, sulla sinistra sono disponibili le seguenti categorie:

- **Antivirus**
- **Controllo Privacy**
- **Firewall**
- **Antispam**
- **Controllo Genitori**
- **Tune Up**

- **Backup**
- **Aggiornamento**

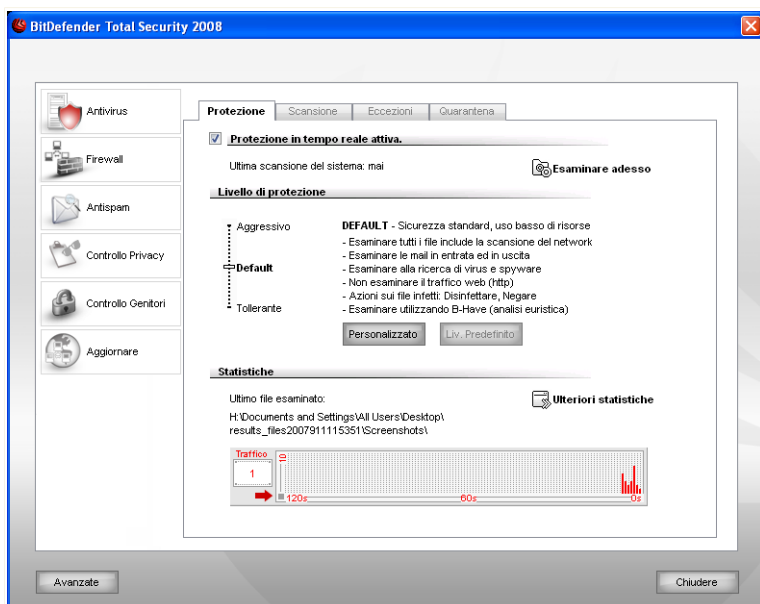
Per ogni categoria c'è una lista di eventi disponibile. Ogni evento viene con la seguente informazione: una breve descrizione, l'azione intrapresa da BitDefender quando è successo, e la data ed ora in cui è successo. Se volete trovare ulteriori informazioni su un particolare evento della lista, cliccateci due volte sopra.

Cliccare su **Cancellare Registro** se si desidera rimuovere tutti i vecchi registri, oppure **Aggiornare** per assicurarsi di visualizzare i registri più recenti.

Amministrazione della Sicurezza Avanzata

6. Iniziando

Sicurezza Totale BitDefender 2008 arriva con un console di configurazione centralizzato, il quale vi permette la configurazione avanzata e la gestione di BitDefender.

Per accedere al console di configurazione, cliccare sul link **Impostazioni**, situato in fondo al Centro di Sicurezza.

Console di Configurazione

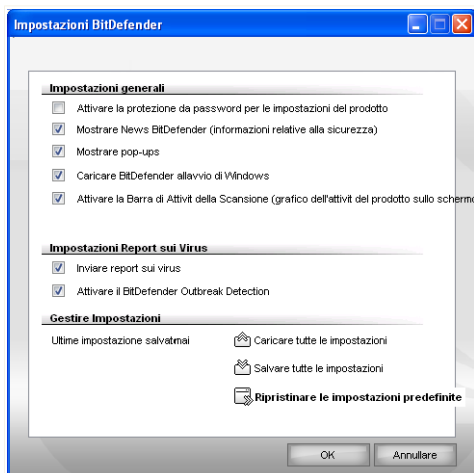
Il console di configurazione è organizzato in moduli: **Antivirus**, **Firewall**, **Antispam**, **Controllo Privacy**, **Controllo Genitori** e **Aggiornamento**. Questo permette di gestire facilmente BitDefender basandosi sul tipo di problema di sicurezza.

Sulla parte sinistra del console di configurazione si trova il selettore dei moduli:

- Antivirus - in questa sezione potete configurare il modulo **Antivirus**.
- Firewall - in questa sezione potete configurare il modulo **Firewall**.

- Antispam - in questa sezione potete configurare il modulo **Antispam**.
- Controllo Genitori - in questa sezione potete configurare il modulo **Controllo dei Genitori**.
- Controllo Genitori - in questa sezione potete configurare il modulo **Controllo dei Genitori**.
- Aggiornamento - in questa sezione puoi configurare il modulo **Aggiornamento**.

6.1. Configurazione delle Impostazioni Generali

Per configurare e gestire le impostazioni generali di Sicurezza Totale BitDefender 2008, cliccare su **Avanzate**. Apparirà una nuova finestra.

Impostazioni Generali

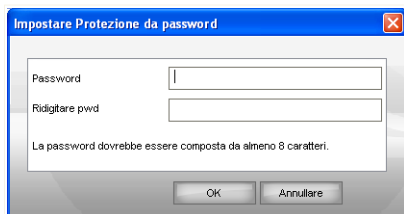
Da qui è possibile impostare il comportamento generale di BitDefender. BitDefender è caricato automaticamente all'avvio di Windows e successivamente minimizzato nella barra strumenti.

6.1.1. Impostazioni Generali

- **Abilita la protezione password per le impostazioni del prodotto** - consente l'impostazione di una password per proteggere la configurazione della Cconsole di Gestione BitDefender.

Nota
Se non siete l'unica persona ad utilizzare questo computer, consigliamo di proteggere le vostre Impostazioni BitDefender con una password.

Selezionando questa opzione, apparirà la finestra:

Inserisci password

Digitare la password nel campo **Password**, quindi re-inserirla campo **Ridigitare pwd** e selezionare **OK**.

Da adesso se si desidera cambiare le opzioni di configurazione di BitDefender, vi verrà richiesta la password.

Importante
Se si dimentica la password, è necessario riparare il prodotto per modificare la configurazione BitDefender.

- **Ricezione notifiche di sicurezza** - riceve di volta in volta, dai server BitDefender, segnalazioni di sicurezza relative alla diffusione di nuovi virus.
- **Mostra pop-ups (attiva la schermata delle note)** - mostra finestre a tendina relative allo stato del prodotto.
- **Caricamento di BitDefender all'avvio di Windows** - esecuzione automatica di BitDefender all'avvio del sistema. Si raccomanda di lasciare questa opzione selezionata.
- **Attivare barra di attività della scansione (grafico dell'attività del prodotto sullo schermo)** - attiva / disattiva la Barra di attività della Scansione.

6.1.2. Impostazioni Report sui Virus

- **Inviare Report sui Virus** - invia ai Laboratori BitDefender i report relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.

  I report non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno solo il nome del virus e verranno utilizzate unicamente per creare report statistici.

- **Attivare Outbreak Detection BitDefender** - invia ai Laboratori BitDefender i report relativi al potenziale scoppio di un virus.

  I report non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno esclusivamente il nome del virus e verranno utilizzate per creare report statistici.

6.1.3. Gestione Impostazioni

Facendo un click su **Salva tutte le impostazioni** / **Salva tutte le impostazioni** vengono salvate le impostazioni da voi eseguite per il BitDefender in una locazione desiderata. In questo modo potrete utilizzare dopo avere re-installato o riparato il vostro BitDefender.

Importante
Solo gli utenti con diritti di amministrazione possono salvare e caricare le impostazioni.

Per caricare le impostazioni di default, cliccate su **Ripristina Impostazioni di Default**.

6.2. Utilizzo della Barra delle Attività di Scansione

La **Barra delle Attività di Scansione** è una visualizzazione grafica delle attività di scansione sul vostro sistema.

Le barre verdi (**Zona File**) indicano il numero di files esaminati al secondo in una scala da 0 a 50.

Le barre rosse visualizzate nella **Zona Rete** mostrano il numero di Kbyte trasferiti (inviati e ricevuti da Internet) al secondo, in una scala da 0 a 100.

Barra delle Attività

Nota
La Barra attività di Scansione vi avviserà con una croce rossa sopra l'area corrispondente quando la protezione in tempo reale o il Firewall sono disattivati (**Zona File** o **Zona Rete**).

Potete usare la**Barra delle attività di scansione** per esaminare degli oggetti. Fare semplicemente il drag & drop degli oggetti che volete esaminare sulla barra.

Nota
Per ulteriore informazione, vi preghiamo di riferirvi a «*Scansione Seleziona e Trascina*» (p. 89).

Quando non si vuole vedere la visualizzazione grafica, è sufficiente fare un click con il tasto destro del mouse sulla stessa e selezionare**Nascondi**. Per nascondere completamente questa finestra, cliccare su **Avanzate** nel console delle impostazioni e deselezionare la casella corrispondente a **Attiva la Barra delle attività di scansione (grafica dell'attività del prodotto sullo schermo)**.

7. AntiVirus

BitDefender protegge il vostro computer da ogni tipo di minaccia malware (virus, troiani, spyware, rootkit ed altro).

Oltre alla classica scansione basata sulle impronte malware, BitDefender eseguirà inoltre una scansione euristica dei file esaminati. L'obiettivo della scansione euristica è quello di identificare nuovi virus, basata su determinate caratteristiche ed algoritmi, prima che un virus venga definito. Possono apparire messaggi di falso allarme. Quando viene rilevato, un file di questo tipo è classificato come sospetto. In questi casi consigliamo di inviare il file ai laboratori BitDefender per essere esaminato.

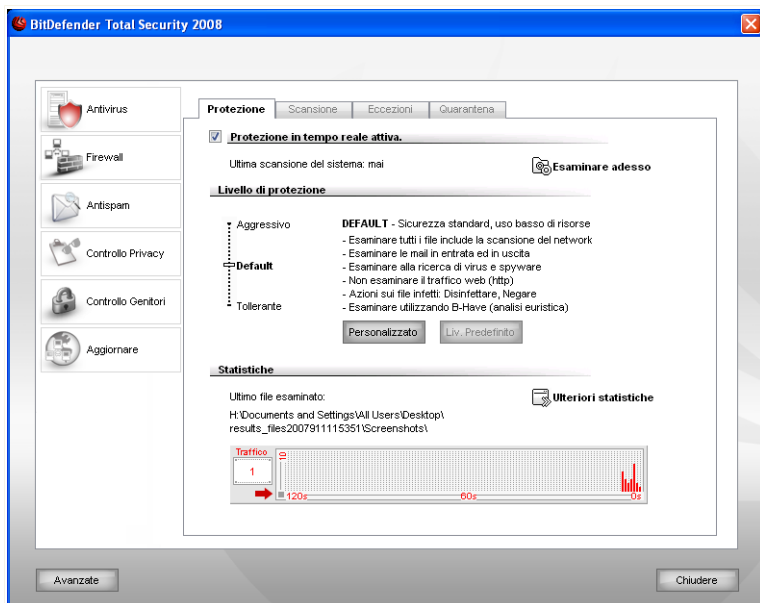
La protezione che BitDefender vi offre è divisa in due categorie:

- **Scansione all'accesso** - impedisce alle minacce malware di entrare nel vostro sistema. Viene anche chiamata protezione in tempo reale - i file vengono esaminati durante il loro utilizzo - all'accesso. BitDefender esaminerà, ad esempio, un documento word quando verrà aperto, ed una mail quando verrà ricevuta.
- **Scansione a richiesta** - permette di rilevare e di rimuovere malware già residente nel vostro sistema. Si tratta della classica scansione dei virus avviata dall'utente – si sceglie quale drive, cartella o file BitDefender deve esaminare e BitDefender li esamina – a richiesta. I processi della scansione vi permettono di creare routine di scansione personalizzate e la loro esecuzione può essere programmata con una cadenza regolare.

La sezione **Antivirus** di questa guida all'utente contiene i seguenti argomenti:

7.1. Scansione all'accesso

Scansione all'accesso, conosciuta anche come protezione in tempo reale, mantiene il vostro computer protetto da ogni tipo di minaccia malware mediante la scansione di tutti i file acceduti, le mail e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Per configurare e monitorare la protezione in tempo reale, cliccare su **Antivirus Shield** nel console delle impostazioni. Apparirà la finestra seguente:

Virus Shield

Importante
Per impedire ai virus di infettare il vostro computer, tenere abilitato il **Virus Shield**.

Nella parte inferiore della sezione è possibile osservare le statistiche **Virus Shield** relative ai file e ai messaggi e-mail. Selezionare **Ulteriori Statistiche** se si desidera visualizzare una finestra maggiormente esplicativa.

Per avviare una scansione veloce del sistema, cliccare su **Esaminare Adesso**.

7.1.1. Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

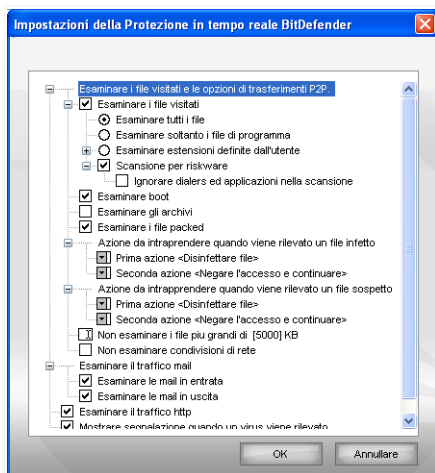
Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Copre le necessità di sicurezza di base. Il livello di consumo delle risorse è molto basso. I programmi e i messaggi di posta in arrivo sono scansionati solo alla ricerca di virus. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/vieta l'accesso.
Default	Offre una sicureza standard. Il livello di consumo delle risorse è basso. Tutti i file e i messaggi di posta in arrivo ed in uscita sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/vieta l'accesso.
Aggressiva	Offre una sicurezza alta. Il livello di consumo delle risorse è moderato. Tutti i file, e i messaggi e-mail in entrata ed in uscita ed il traffico web sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/vieta l'accesso.

Per applicare le impostazioni di protezione in tempo reale di default cliccare su **Livello di Default**.

7.1.2. Livello di Protezione Personalizzato

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Potete personalizzare la **Real-time protection** cliccando **Custom level**. Apparirà la seguente finestra:

Impostazioni Virus Shield

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows.

Nota

Selezionare la casella con "+" per aprire una opzione oppure la casella con "-" per chiudere una opzione.
Si può vedere come alcune opzioni di scansione, nonostante appaia il segno "+", non possano essere aperte. Il motivo è che queste opzioni non sono ancora state selezionate.
Si può notare che sarà possibile aprirle una volta selezionate.

- **Scansione dei file in accesso e dei transferimenti P2P** - esamina i file acceduti e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Successivamente selezionare il tipo di file che si desidera esaminare.

Opzione		Descrizione
Esamina i files acceduti	**Esamina tutti i files**	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.

Opzione		Descrizione
	Soltanto i programmi ed i documenti	Verranno esaminati solo i file di programma, con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` e `.nws`.
	Esamina le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Queste estensioni devono essere separate da ";".
	Scansione per riskware	Esamina alla ricerca di riskware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva. Selezionare **Salta dialers e applicazioni dalla scansione** se si desidera escludere questi tipo di files dalla scansione.
Scansione del settore di avvio		Esamina il settore di avvio del sistema.
Esamina gli archivi		Verranno esaminati gli archivi acceduti. Abilitando questa opzione, il computer sarà più lento.
Esamina i programmi impaccati		Verranno esaminati tutti i file impaccati.
Prima azione		Seleziona dal menù delle opzioni la prima azione da intraprendere su files infetti o sospetti:
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
	Ripulisci file	Disinfetta i file infetti.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.

Opzione		Descrizione
	Muovi il file in quarantena	Sposta i file infetti nella zona di quarantena.
Seconda azione		Seleziona la seconda azione dalle opzioni da intraprendere sui files infetti, nel caso in cui la prima fallisse.
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
	Muovi il file in quarantena	Sposta i file infetti nella zona di quarantena.
Non esaminare i files più grandi di [x] Kb		Digitare la dimensione massima dei files da esaminare. Se la dimensione è pari a 0 Kb, tutti i files verranno esaminati.
Non esaminare condivisioni di rete		Se questa opzione è attiva, BitDefender non esaminerà le condivisioni di rete, permettendo un accesso alla rete più veloce. Vi consigliamo di attivare questa opzione solo se la rete della quale fate parte è protetta con una soluzione antivirus.

- **Esamina il traffico e-mail** - tutti i messaggi e-mail vengono esaminati.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Esamina le e-mail in ingresso	Tutte le e-mail in ingresso vengono esaminate.
Esamina le e-mail in uscita	Tutte le e-mail in uscita vengono esaminate.

- **Esamina il traffico http** - tutto il traffico http viene esaminato.
- **Mostra avviso se viene rilevato un virus** - verrà visualizzata una finestra di avviso ogni volta che verrà rilevato un virus in un file o in un messaggio e-mail.

  In presenza di un virus, si aprirà una finestra contenente il nome del virus, e che permetterà di selezionare un azione sul file infetto adottata dal BitDefender, e un

link al sito BitDefender dove sarà possibile trovare ulteriori informazioni al riguardo. Per una e-mail infetta, la finestra di allerta contiene anche informazioni sul mittente e il destinatario.

Nel caso in cui un file sospetto è rilevato, potete lanciare una procedura dalla finestra di allerta che vi aiuterà a trasmettere il file ai Laboratori BitDefender per una ulteriore analisi. È possibile scrivere dalla vostra e-mail per ricevere informazioni relative a questo report.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

7.1.3. Disattivazione Virus Shield

Se volete disattivare la protezione in tempo reale, apparirà la seguente finestra di avviso:

Disattivare Virus Shield

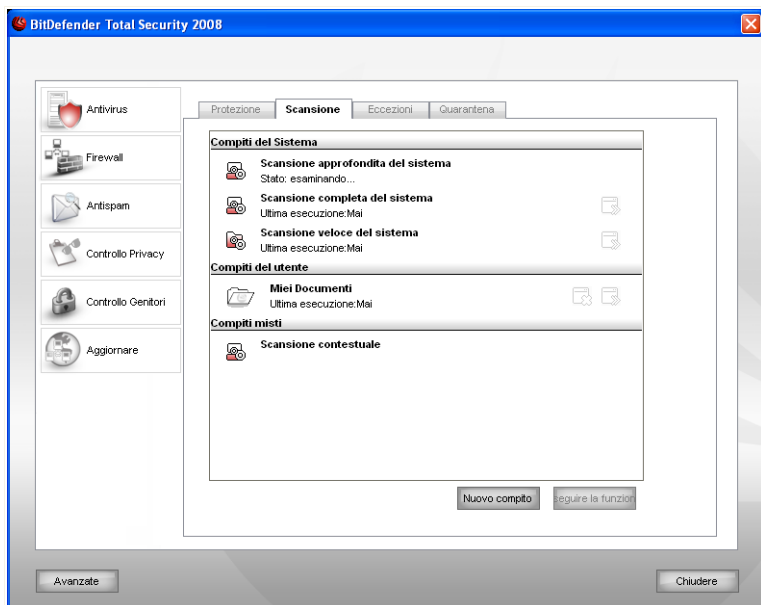
Dovrete confermare la vostra scelta selezionando dal menu, per quanto tempo volete disattivare la protezione in tempo reale. Potete disattivarla durante 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento
Questa è una questine di sicurezza critica. Vi consigliamo di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale non è attiva, non sarete protetti dalle minacce malware.

7.2. Scansione a richiesta

L'obiettivo principale di BitDefender è di mantenere il vostro computer privo di virus. Ciò avviene principalmente tenendo lontani i nuovi virus dal vostro computer ed esaminando i vostri messaggi e-mail e qualsiasi nuovo file scaricato o copiato sul vostro sistema.

Esiste il rischio che un virus sia già contenuto nel vostro sistema, addirittura prima dell'installazione di BitDefender. Questo è il motivo per cui suggeriamo di effettuare una scansione sul vostro computer alla ricerca di virus residenti dopo aver installato BitDefender. E' inoltre una buona idea effettuare frequentemente una scansione del vostro computer, alla ricerca di virus.

Per configurare ed avviare la scansione a richiesta, cliccare su **Antivirus>Scansione** nel console di configurazione. Apparirà la finestra seguente:

Impostazioni della Scansione

La scansione a richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scasione e gli ooggetti da esaminare. Potete esaminare il vostro computer in qualsiasi momento, eseguendo le funzioni predefinite oppure le vostre proprie (definite dall'utente). Potete anche programmarle per venire eseguite con cadenza regolare oppure quando il sistema risulti così ozioso di non interferire con il vostro lavoro.

7.2.1. Impostazioni della Scansione

BitDefender ha tante funzioni, create per default, che coprono i problemi di sicurezza comuni. Voi potete anche creare le vostre funzioni di scansione personalizzate.

Ogni funzione o compito ha una finestra delle **Proprietà** che vi permette di configurare il compito e di vedere i risultati della scansione. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Configurare un Compito di Scansione»* (p. 78).

Vi sono tre categorie di compiti di scansione:

- **Impostazione del Sistema** - contiene la lista delle impostazioni di default. Sono disponibili le impostazioni seguenti:

Compito di default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione Completa del Sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione Veloce del Sistema	Esamina le cartelle `Windows`, `Program Files` e `All Users`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.

Nota
Poichè le funzioni **Scansione del sistema approfondita** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi vi consigliamo di eseguire questi compiti con priorità bassa, o meglio, quando il vostro sistema risulti ozioso.

- **Impostazione Utente** - contiene le impostazioni definite dall'utente.

  Viene fornita una funzione chiamata `My Documents`. Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`,

`Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

- **Compiti misti** - contiene un elenco di compiti di scansione misti. Questi compiti di scansione si riferiscono a tipi di scansione alternativi che non possono essere eseguiti da questa finestra. Potete solo modificare le loro impostazioni o vedere i report delle scansioni.

Alla destra di ogni impostazione sono disponibili tre pulsanti:

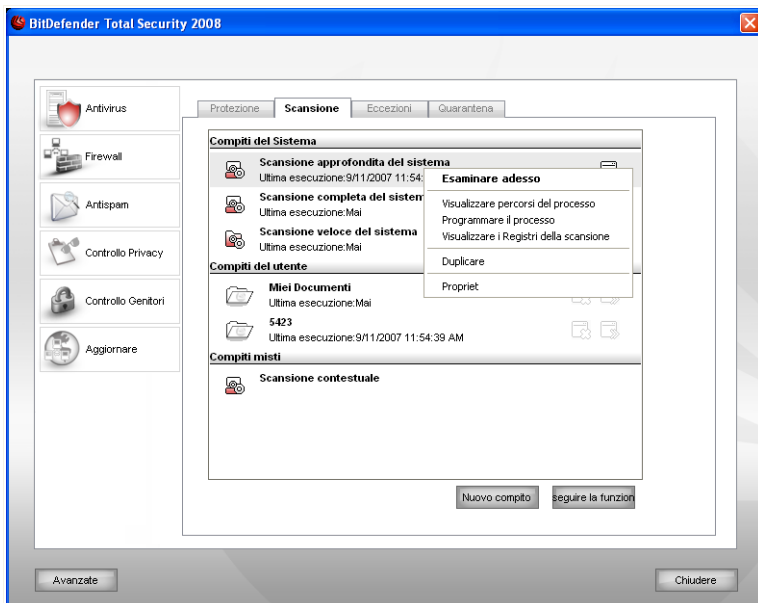
- **Funzione Programmata** - indica che la funzione selezionata è programmata per essere successivamente utilizzata. Cliccare su questo tasto per aprire la sezione Programmatore nella finestra delle **Proprietà**, dove è possibile visualizzare la programmazione delle funzioni e modificarla.
- **Cancella** - rimuove la funzione selezionata.

Nota
Non disposnibile per compiti di sistema. Non potete rimuovere un compito di sistema.

- **Scansiona Adesso** - esegue la funzione selezionata, iniziando una scansione immediata.

Alla sinistra di ogni funzione potrete vedere il tasto delle **Proprietà**, che vi permette di configurare i compiti e visualizzare i registri della scansione.

7.2.2. Utiulizzo del Menu Rapido

Un menu rapido è

Menu Rapido

disponibile per ciascun compito. Cliccare col pulsante destro del mouse sul compito selezionato per aprirlo.

Nel menù collegato sono disponibili i seguenti comandi:

- **Scan Now** - esegue la funzione selezionata, avviando immediatamente una scansione.
- **Cambiare il Target di Scansione** - apre la sezione Percorso Scansione nella finestra delle **Proprietà**, dove potete cambiare il target di scansione per i compiti selezionati.

Nota

Nel caso di funzioni del sistema, questa opzione viene sostituita da **Mostrare Percorsi delle Funzioni**, dato che potete vedere solo il loro target di scansione.

- **Funzione Programmazione** - apre la sezione Programmazione nella finestra delle **Proprietà**, dove potete programmare il compito selezionato.
- **Visualizzare i Registri di Scansione** - apre la sezione Registri della Scansione nella finestra delle **Proprietà**, dove potete vedere i report generati dopo che il compito selezionato è stato eseguito.
- **Duplicare** - duplica i compiti selezionati.

Nota
Ciò è utile quando si creano nuovi compiti, in quanto potete modificare le impostazioni del compito duplicato.

- **Cancella** - cancella i compiti selezionati.

Nota
Non disposnibile per compiti di sistema. Non potete rimuovere un compito di sistema.

- **Proprietà** - apre la sezione Visione generale nella finestra delle **Proprietà**, dove potete cambiare le impostazioni del compito selezionato.

Nota
Data la loro particolare natura, solo le opzioni **Proprietà** e **Visualizzare Registri Scansione** sono disponibili per la categoria delle funzioni **Compiti Misti**.

7.2.3. Creazione delle Funzioni di Scansione

Per creare un compito di scansione, utilizzare uno di questi metodi:

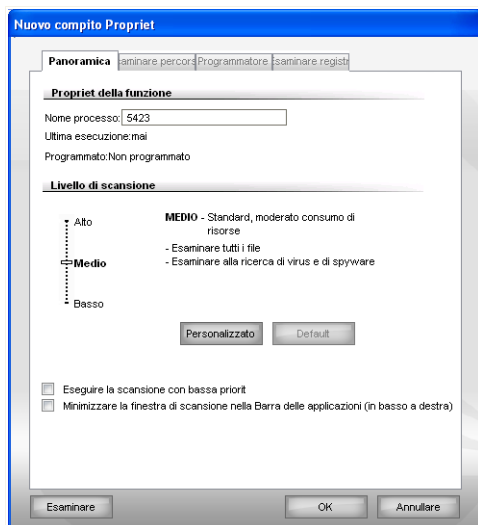
- Duplicare un compito esistente, rinominarlo ed apportare le modifiche necessarie nella finestra delle Proprietà;
- Cliccare **Nuovo Compito** per creare un nuovo compito e configurarlo.

7.2.4. Configurare un Compito di Scansione

Ogni compito di scansione ha la sua propria finestra delle **Proprietà**, dove potete configurare le opzioni di scansione, impostare il target della scansione, programmare il compito o vedere i report. Per aprire questa finestra cliccare sul tasto **Aprire**, posto sulla destra della funzione (o cliccare con il tasto destro sulla funzione e quindi cliccare **Aprire**).

Nota
Per ulteriori informazioni sulla visualizzazione dei registri e sulla funzione **Registri**, vi preghiamo di riferirvi a *«Visualizzazione dei Registri di Scansione»* (p. 94).

Configurazione delle Impostazioni di Scansione

Per configurare le opzioni di scansione di un compito specifico, cliccare con il tasto destro e selezionare**Proprietà**. Apparirà la finestra seguente:

Informazioni generali sul prodotto BitDefender™

Qui potete vedere le informazioni sul compito (nome, ultima esecuzione e stato della programmazione) ed impostare le impostazioni di scansione.

Scelta del Livello di Scansione

Potete facilmente configurare le impostazioni di scansione scegliendo il livello di scansione. Trascinare l'inidcatore sulla barra per impostare l'appropriato livello di scansione.

Ci sono 3 livelli di scansione:

Livello di protezione	*Descrizione*
Basso	Offre un'efficienza di rilevamento ragionevole. Il livello di consumo delle risorse è basso. Vengono esaminati alla ricerca di virus solo i programmi. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica.
Medio	Offre una buona efficienza di rilevamento. Il livello di consumo delle risorse è moderato. Tutti i file vengono esaminatinati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizata anche l'analisi euristica.
Alto	Offre un'alta efficienza di rilevamento. Il livello di consumo di risorse è alto. Tutti i file e gli archivi vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.

È anche disponibile una serie di opzioni generali per il processo di scansione:

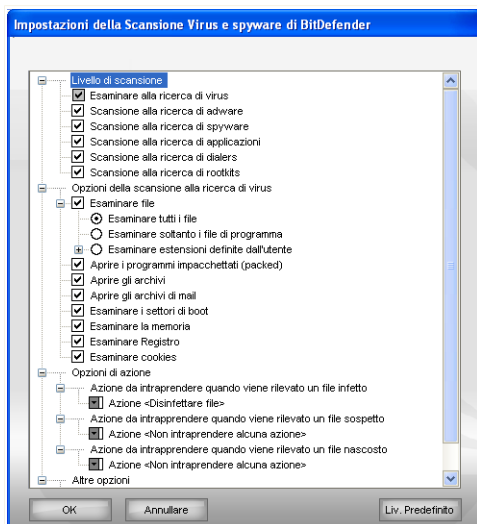
Opzione	*Descrizione*
Esegui la scansione con priorità bassa	Riduce la priorità del processo di scansione. Consentirete ad altri programmi di essere più veloci ed incrementerete il tempo necessario per terminare il processo di scansione.
Ridurre a icona la finestra di scansione nella barra degli strumenti	Riduce a icona la finestra di scansione sulla barra degli strumenti. Eseguire un doppio clic sull'icona di BitDefender per riaprirla.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

Personalizzazione del Livello di Scansione

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare

solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Cliccare su **Personalizza** per impostare le vostre opzioni di scansione. Si aprirà una nuova finestra.

Impostazioni di Scansione

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows. Selezionare la casella con "+" per aprire una opzione oppure la casella con "-" per chiudere una opzione.

Le opzioni di scansione sono raggruppate in quattro categorie:

- **Livello di Scansione**
- **Opzioni di scansione virus**
- **Opzioni delle Azioni**
- **Altre opzioni**

- Specificare il tipo di malware che volete che Bit Defender analizzi, selezionando le opzioni appropriate dalla categoria **Livello di scansione**.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. BitDefender rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansione applicazione	Esamina le applicazioni (`.exe` e i file `.dll`).
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.

- Specificare il tipo di oggetti che devono essere scansionati (archivi, messaggi e-mail e così via) e altre opzioni. Ciò avviene attraverso la selezione di determinate opzioni dalla categoria **Opzioni di scansione virus**.

  Sono disponibili le seguenti opzioni:

Opzione		Descrizione
Scansione files	**Esamina tutti i files**	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.
	Soltanto i programmi ed i documenti	Saranno esaminati solamente i files di programma. Conseguentemente solo i files con le seguenti estensioni: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`;

Opzione	Descrizione
	php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws.
Esamina le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Queste estensioni devono essere separate da ";".
Apri i programmi impaccati	Scansiona i files impaccati.
Apri gli archivi	Scansiona l'interno degli archivi.
Aperrtura degli archivi e-email	Eseguire la scansione all'interno degli archivi di posta.
Scansione dei settori di avvio	Esamina il settore di avvio del sistema.
Scansione della memoria	Scansiona la memoria alla ricerca di virus e altro malware.
Scansione registro	Scansione di voci di registro.
Scansionare cookies	Esamina i files cookie.

- Specificare l'azione da intraprendere sui file infetti, sospetti o nascosti rilevati nella categoria **Opzioni di Azione**. Potete specificare una diversa azione per ogni categoria.
  - Selezionare l'azione da intraprendere sui file infetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Nessuno(log oggetti)	Nessuna azione verrà eseguita sui file infetti. Questi files appariranno nel file di report.
Disinfetta i files	Disinfetta i file infetti.
Cancella i files	Cancella immediatamente i file infetti, senza alcun avviso.
Muovere i files in Quarantena	Sposta i file infetti nella zona di quarantena.

  - Selezionare l'azione da intraprendere sui file sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Nessuno(log oggetti)	Nessuna azione verrà eseguita sui file sospetti. Questi files appariranno nel file di report.
Cancella i files	Cancella immediatamente i files sospetti, senza alcun avviso.
Muovere i files in Quarantena	Sposta i file sospetti nella zona di quarantena.

Nota
La Scansione euristica ha rilevato dei file sospetti. Vi consigliamo di inviarli al laboratorio di BitDefender.

- Selezionare l'azione da intraprendere sugli oggetti nascosti (rootkits) rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Nessuno(log oggetti)	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Muovere i files in Quarantena	Sposta i file nascosti nella zona di quarantena.
Rendere visibili	Rivela i file nascosti in modo che possano essere visti.

Nota
Se sceglliete di ignorare i file rilevati o se l'azione selezionata fallisce, dovrete scegliere un'azione nell'assistente di scansione

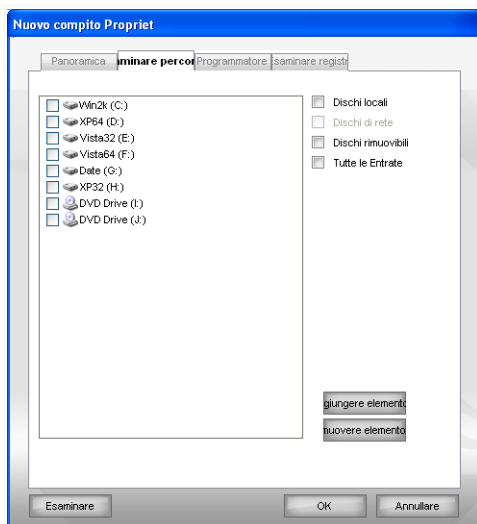
- Per far sì che venga richiesta di inviare tutti i file sospetti al laboratorio BitDefender dopo che il processo di scansione sia stato completato, selezionare **inviare tutti i file sospetti al laboratorio BitDefender** nella categoria **Altre Opzioni**.

Se clicchi su **Predefinito** verranno applicate le impostazioni di default. Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

Impostazione del Target di Scansione

Nota

Non potete modificare il target di scansione delle funzioni di scansione dalla categoria**Funzioni del Sistema**. Potete solo visualizzare il target di scansione.

Per impostare il target di scansione di un compito di scansione spedifico, cliccare con il tasto destro sul compito e selezionare **Modificare Target di Scansione** (o **Mostrare Percorsi delle funzioni** per le funzioni di sistema, per visualizzare il loro target). Apparirà la finestra seguente:

Target di Scansione

Potete vedere la lista di dischi locali, di rete e rimuovibili, ed anche i file e cartelle aggiunti in precedenza, se ci sono. Tutti glòi oggetti selezionati verranno esaminati all'esecuzione della funzione.

La sezione contiene i seguenti pulsanti:

- **Aggiungere Oggetto (i)** - apre una finestra di visualizzazione dove è possibile selezionare il (i) file / cartella(e) che si desidera esaminare.

Nota

Potete anche selezionare e trascinare files/cartelle da aggiungere all'elenco.

- **Cancellare Oggetti** - rimuove il (i) file / cartella(e) precedentemente selezionati dall'elenco degli oggetti da esaminare.

Nota

Possono essere cancellati solo i file(s)/cartelle aggiunti successivamente ma non quelli "visti" automaticamente da BitDefender.

Oltre ai pulsanti sopra esposti, ci sono anche alcune opzioni che permettono la selezione veloce della locazione di scansione.

- **Dischi locali** - per esaminare i drives locali.
- **Dischi di rete** - per esaminare tutti i drives di rete.
- **Drives Rimovibili** - per esaminare i drives removibili (CD-ROM, floppy-disk).
- **Tutti gli elementi** - per esaminare tutti i drives, indipendentemente dal fatto che siano locali, sulla rete o rimovibili.

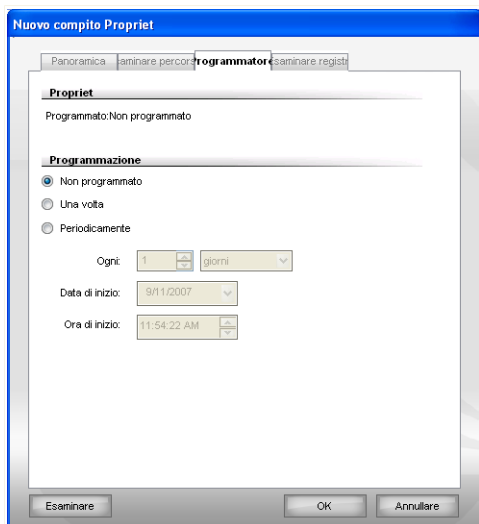
Nota

Se desiderate eseguire una scansione di tutto il vostro computer alla ricerca di virus, selezionare la casella corrispondente a **Tutti gli elementi**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

Programmazione delle Funzioni di Scansione

Una scansione completa può richiedere un certo tempo e agisce meglio se vengono chiusi tutti gli altri programmi. La miglior cosa da fare è programmare la scansione nel momento in cui il vostro computer non viene utilizzato.

Per visualizzare la programmazione di un compito specifico o per modificarla, cliccare con il tasto destro e selezionare **Programmare Funzione**. Apparirà la finestra seguente:

Programmatore

Potete vedere la programmazione delle funzioni, se ci sono.

Quando programmate un compito, dovete scegliere una delle seguenti opzioni:

- **Non programmata** - lancia la funzione solo quando richiesta dall'utente.
- **Una volta** - lancia la scansione solo una volta, in un certo momento. Specificare la data e l'ora di avvio nel campo **Start Date/Time**.
- **Periodicamente** - lancia la scansione periodicamente, a certi intervalli di tempo (ore, giorni, settimane, mesi, anni) iniziando da una certa data ed ora specificate dall'utilizzatore.

  Se si desidera che la scansione venga ripetuta a determinati intervalli, selezionare la casella corrispondente a **Periodicamente** e digitare nel campo **Ogni** il numero di minuti / ore / giorni / settimane / mesi / anni indicando la frequenza del processo. Dovete inoltre specificare la data e l'ora di inizio nel campo **Start Date/Time**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

7.2.5. Oggetti di Scansione

Prima di iniziare il processo di scansione, dovreste assicurarvi che BitDefender sia aggiornato con le impronte malware. Eseguire la scansione usando un database delle impronte obsoleto può impedire BitDefender di rilevare nuovo malware, trovato dopo l'ultimo aggiornamento. Per verificare quando è stato eseguito l'ultimo aggiornamento, cliccare su **Aggiornamento>Aggiornamento** nel console di configurazione.

Nota
Per consentire a BitDefender di eseguire una scansione completa, dovrete chiudere tutti i programmi aperti. In particolare è importatnte chiudere il vostro client di posta (come Outlook, Outlook Express oppure Eudora).

Metodi di Scansione

BitDefender consente quattro tipi di scansione a richiesta:

- Scansione immediata - avvia immediatamente un processo di scansione dal sistema / funzioni utente.
- Scansione contestuale - selezionare un file o una cartella con il tasto destro e selezionare Antivirus BitDefender 2008;
- Scansione Seleziona & Trascina - seleziona & trascina un file o una cartella sopra la Barra delle Attività di Scansione.
- Scansione manuale - Utilizzare Scansione Manuale di BitDefender per selezionare direttamente i file o cartella da esaminare.

Scansione Immediata

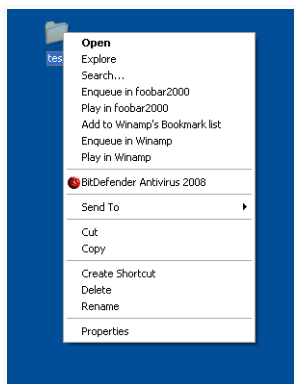
Per eseguire una scansione del vostro computer o di parte di essi potete usare i compiti di scansione di default oppure i vostri propri compiti di scansione. Ciò si chiama scansione immediata

Per eseguire un compito di scansione, utilizzare uno dei seguenti metodi:

- fare doppio click sul compito di scansione desiderato dall'elenco.
- cliccare sul pulsante **Esegui scansione ora** corrispondente al compito.
- selezionare il compito e quindi cliccare su **Esegui Compito**.

Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Scanner di BitDefender.*» (p. 90).

Scansione Contestuale

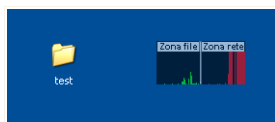
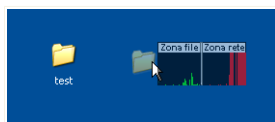
Per esaminare un file o cartella senza configurare un nuovo compito di scansione, si può usare il menu contestuale. ciò si chiama scansione contestuale

Scansione Contestuale

Cliccare con il tasto destro sul file o la cartella che si desidera esaminare e selezionare **Antivirus BitDefender 2008**.

Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Scanner di BitDefender.»* (p. 90).

E' possibile modificare e vedere il file di report dalla finestra delle **Proprietà** del **Menu Scansione Contestuale**.

Scansione Seleziona e Trascina

Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.

Trascinare il file

Abbandonare il file

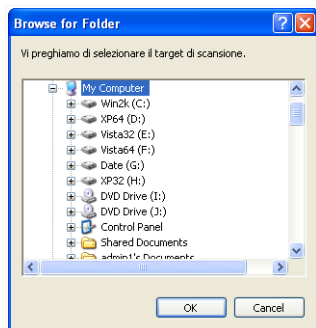
Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a «Scanner di BitDefender.» (p. 90).

Scansione Manuale

La scansione manuale consiste in selezionare direttamente l'oggetto da esaminare, utilizzando l'opzione Scansione Manuale BitDefender dal gruppo di programmi BitDefender nel Menu di Avvio.

Nota
La scansione manuale è molto utile, poichè può essere eseguita anche quando Windows lavora in Modalità Provvisoria.

Per selezionare l'oggetto da esaminare, nel menu Avvio di Windows, seguire il percorso **Avvio** → **Programmi** → **BitDefender 2008** → **Scansione Manuale di BitDefender**.

Apparirà la finestra seguente:

Scansione Manuale

Scegliere l'oggetto che si desidera esaminare e cliccare **OK**.

Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a «Scanner di BitDefender.» (p. 90).

Scanner di BitDefender.

Quando il processo di scansione a richiesta si avvierà, lo Scanner BitDefender apparirà. Seguire la procedura di tre passi per completare il processo di scansione.

Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.

Scansione

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Nota
La durata del processo dipende dalla complessità della scansione.

Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

Potete fermare la scansione in qualsiasi momento, cliccando su**Fermare**. Verrete portati all'ultimo passo dell'assistente.

Nota
Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di sottoporli al Lab BitDefender.

Attendere che BitDefender finisca la scancione.

Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.

Le seguenti opzioni possono comparire nel menu:

Azione	*Descrizione*
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati.

Azione	Descrizione
Disinfettare	Disinfetta i file infetti.
Eliminare	Elimina i file infetti.
Mostrare	Rende visibili i file nascosti

Click **Risolvere i problemi** per applicare le azioni specificate.

Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.

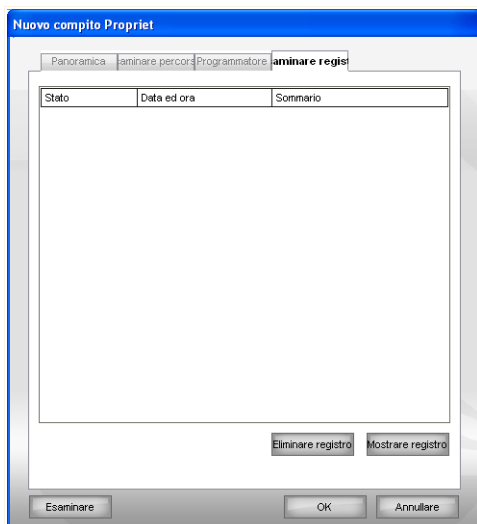
Sommario

E' possibile visualizzare il sommario dei risultati.

Il file di report viene automaticamente salvato nella sezione Registri della finestra delle **Proprietà** di ogni funzione.

Avvertimento
Se ci sono problemi non risolti, vi consigliamo di contattare il Team di suppoto di BitDefender su www.bitdefender.com.

7.2.6. Visualizzazione dei Registri di Scansione

Per visualizzare i risultati della scansione una volta completato un compito di scansione, cliccare con il tasto destro sul compito e selezionare **Visualizzare Registri di Scansione**. Apparirà la finestra seguente:

Registri di Scansione

Qui potete vedere i file di report generati ogni volta che il compito è stato eseguito. Ciascun file ha allegate informazioni sul suo stato (pulito/infetto), la data e l'ora in cui la scansione è stata eseguita ed un riassunto (scansione terminata).

Sono disponibili due pulsanti:

- **Mostrare registro** - per visualizzare il file di report selezionato;
- **Cancellare registro** - per cancellare il file di report selezionato.

Inoltre, per vedere o cancellare un file, cliccare con il tasto destro sul file e selezionare l'opzione corrispondente dal menu rapido.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

7.3. Oggetti esclusi dalla Scansione

Ci sono dei casi in cui si può avere bisogno di escludere certi file dalla scansione. Ad esempio, si può volere escludere un file di testo EISCAR dalla scansione all'accesso, oppure i file `.avi` dalla scansione a richiesta.

BitDefender permette di escludere oggetti dalle scansioni all'accesso ed a richiesta, o da entrambi. Questa caratteristica cerca di ridurre i tempi di scansione e di evitare le interferenze con il vostro lavoro.

Due tipi di ggetti possono essere esclusi dalla scansione:

- **Percorsi** - Il file o cartella (inclusi tutti gli oggetti che essi contiene) indicato da un percorso specifico verrà escluso dalla scansione.
- **Estensioni** - tutti i file che hanno una specifica estensione verranno esclusi dalla scansione.

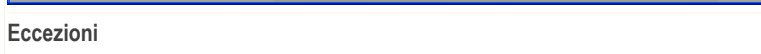
Nota
Gli oggetti esclusi dalla scansione all'accesso non verranno esaminati, non importa se sono visitati da voi o da un'applicazione.

Per visualizzare e gestire gli oggetti esclusi dalla scansioen, cliccare **Antivirus>Eccezioni** nel console di configurazione. Apparirà la finestra seguente:

Eccezioni

Si possono visualizzare gli oggetti (file, cartelle, estensioni) esclusi dalla scansione. Potete vedere se ogni oggetto è stato escluso dalla scansione all'accesso, dalla scansione a richiesta o da entrambi.

Nota
Le eccezioni qui specificate NON verranno applicate nella scansione contestuale.

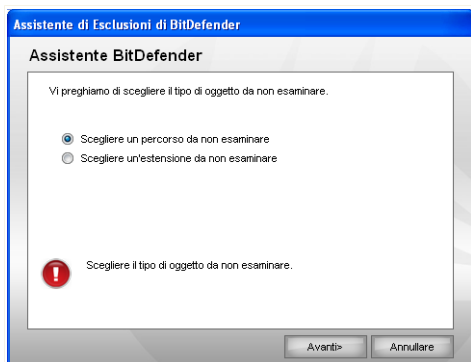
Per rimuovere un'entrata dalla tabella, selezionarla e cliccare il tasto **Eliminare**.

Per modificare un'entrata dalla tabella, selezionarla e cliccare il tasto **Modificare**. Apparirà una nuova finestra dove si potrà modificare l'estensione od il percorso da escludere ed il tipo di scansione dal quale escluderlo, a seconda delle necessità. Apportare le necessarie modifiche e cliccare **OK**.

Nota
Potete anche cliccare con il tasto destro sull'oggetto ed utilizzare le opzioni del menu rapido per modificarlo o eliminarlo.

Potete cliccare su **Ignorare** per ritornare alla situazione precedente alle modifiche effettuate alla tabella delle regole, sempre che non le abbiate salvate cliccando su **Applicare**.

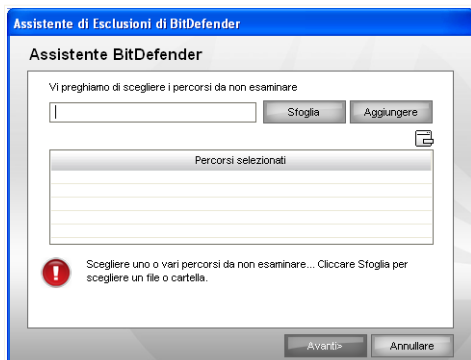
7.3.1. Esclusione dei Percorsi dalla Scansione

Per escludere dei percorsi dalla scansione, cliccare sul tasto **Aggiungere**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione dei percorsi dalla scansione.

Passo 1/3 – Selezione tipo di oggetto

Tipo di Oggetto.

Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Avanti**.

Passo 2/3 – Specificare i percorsi esclusi

Percorsi Esclusi

Per specificare i percorsi da escludere dalla scansione, utilizzare uno dei seguenti metodi:

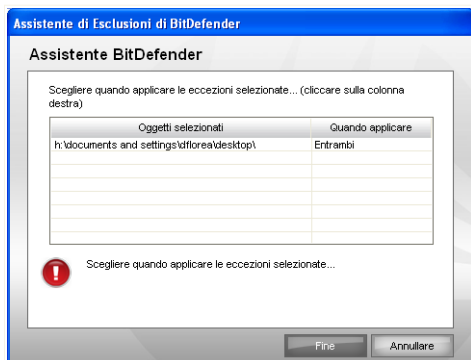
- Cliccare **Sfoglia**, selezionare il file o cartella che volete venga escluso dalla scansione e quindi cliccare su **Aggiungere**.
- Scrivere il percorso che volete venga escluso dalla scansione nel campo modifica e cliccare **Aggiungere**.

Nota
Se il percorso inserito non esiste, comparirà un messaggio di errore. Cliccare **OK** e controllare la validità del percorso.

I percorsi appariranno nella tabella man mano che vengono aggiunti. Potete aggiungere quanti percorsi volete.

Per rimuovere un'entrata dalla tabella, selezionarla e cliccare il tasto **Eliminare**.

Selezionare **Avanti**.

Passo 3/3 – Selezionare tipo di scansione

Tipo di Scansione

Potete vedere una tabella contenente i percorsi da escludere dalla scansione ed il tipo di scansione dal quale vengono esclusi.

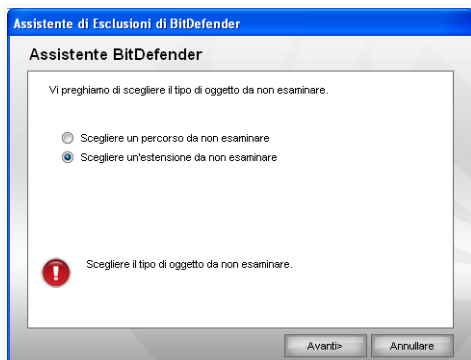
Per default i percorsi selezionati verranno esclusi da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Termina**.

Cliccare **Applica** per salvare le modifiche.

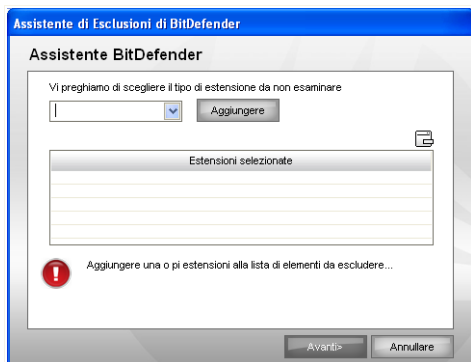
7.3.2. Esclusione delle Estensioni dalla Scansione

Per escludere delle estensioni dalla scansione, cliccare sul tasto **Aggiungere**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione delle estensioni dalla scansione.

Passo 1/3 – Selezione tipo di oggetto

Tipo di Oggetto.

Selezionare l'opzione di escludere una estensione dalla scansione.

Selezionare **Avanti**.

Passo 2/3 – Specificare le estensioni escluse

Estensioni Escluse

Per specificare le estensioni da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Selezionare dal menu l'estensione che volete venga esclusa dalla scansione e quindi cliccare su **Aggiungere**.

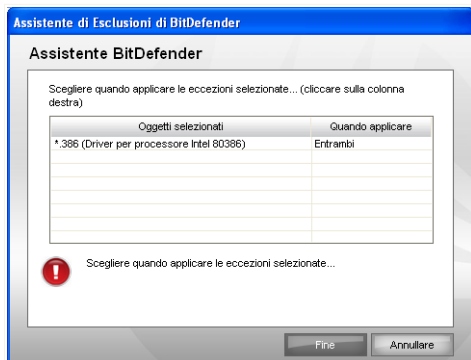
Nota
Il menu contiene un elenco di tutte le estensioni registrate sul vostro sistema. Quando selezionate un'estensione, potrete vedere la sua descrizione, se disponibile.

- Scrivere l'estensione che volete venga esclusa dalla scansione nel campo modifica e cliccare **Aggiungere**.

Le estensioni appariranno nella tabella man mano che vengono aggiunte. Potete aggiungere quante estensioni volete.

Per rimuovere un'entrata dalla tabella, selezionarla e cliccare il tasto **Eliminare**.

Selezionare **Avanti**.

Passo 3/3 – Selezionare tipo di scansione

Tipo di Scansione

Potete vedere una tabella contenente le estensioni da escludere dalla scansione ed il tipo di scansione dal quale vengono escluse.

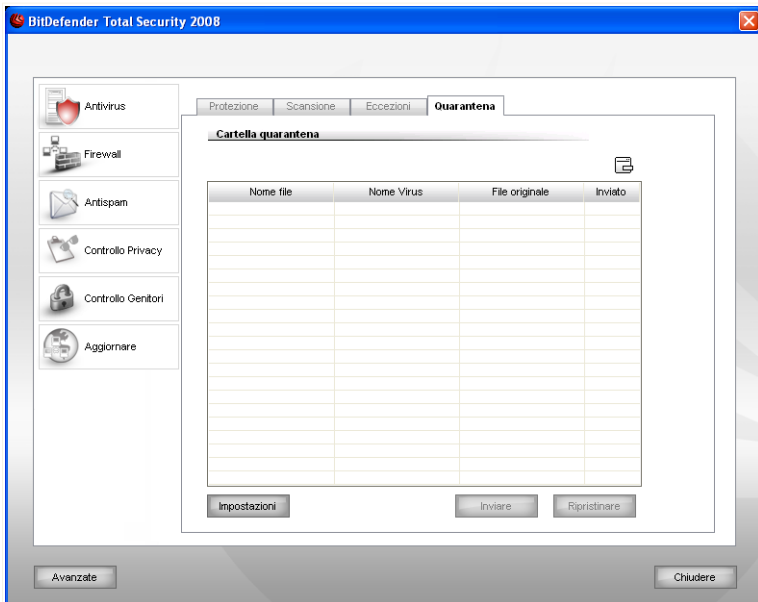
Per default le estensioni selezionate verranno escluse da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Termina**.

Cliccare **Applica** per salvare le modifiche.

7.4. Area di Quarantena

BitDefender consente di isolare i files infetti o sospetti in un'area sicura, chiamata quarantena. Isolando questi files in quarantena, scompare il rischio di essere infettati e contemporaneamente si ha la possibilità di inviare questi files ai Laboratori BitDefender per ulteriori analisi.

Per visualizzare e gestire i file in quarantena e per configurare le impostazioni della quarantena, cliccare su **Antivirus>Quarantena** nel console di configurazione.

Quarantena

7.4.1. Gestione dei File in Quarantena

Come potrete notare, la sezione **Quarantena** contiene un elenco di tutti i files che sono stati isolati fino a quel momento. Ogni file ha allegato il suo nome, la dimensione, la data di isolamento e la data di invio.

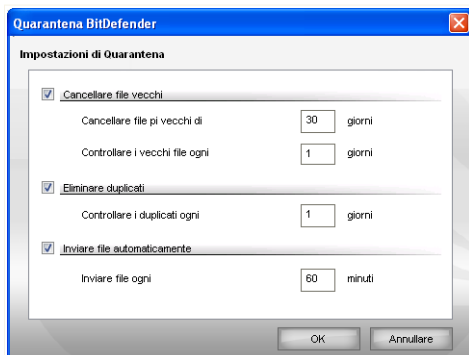
Nota
Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

Per cancellare un file selezionato dalla quarantena, cliccare **Remove**. Se desiderate inviare un file selezionato alla sua ubicazione originale,cliccare **Restore**.

Potet inviare qualsiasi file selzionato dalla quarantena al lab BitDefender clicando su **Invia**.

Menù contestuale. E' disponibile un menu contestuale che vi permette di gestire facilmente i file in quarantena. Sono disponibile le stesse opzioni su menzionate. Potete anche selezionare **Aggiornare** per aggiornare la sezione di Quarantena.

7.4.2. Configurazione delle Impostazioni di Quarantena

Per configurare le impostazioni di quarantena, cliccare su **Impostazioni**. Apparirà una nuova finestra.

Impostazioni di Quarantena

Utilizzando le impostazioni di quarantena, potete configurare BitDefender per eseguire automaticamente le seguenti azioni:

Eliminare i vecchi file. Per eliminare automaticamente i vecchi file, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni dopo i quali i file in quarantena devono essere eliminati e la frequenza con cui BitDefender deve effettuare il controllo dei vecchi file.

Nota
Per default, BitDefender effettuerà il controllo dei vecchi file ogni giorno ed eliminerà i file più vecchi di 10 giorni.

Eliminare duplicati. Per eliminare automaticamente i file duplicati in quarantena, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni tra due controlli consecutivi dei duplicati.

Nota
Per default, BitDefender effettuerà il controllo dei file duplicati in quarantena ogni giorno.

Invio automatico dei file. Per inviare automaticamente i file in quarantena, selezionare l'opzione corrispondente. Dovete specificare la frequenza con cui inviare i file.

Nota
Per default, BitDefender invierà automaticamente i file in quarantena ogni 60 minuti.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

8. Firewall

Il Firewall protegge il vostro computer dai tentativi di connessione non autorizzati sia in entrata che in uscita. E' come una guardia al vostro cancello – manterrà sotto controllo la vostra connessione Internet e terrà traccia di coloro ai quali si concede di accedere ad Internet e di coloro ai quali non è permesso.

Nota
Un firewall è essenziale se si dispone di una banda larga o di una connessione DSL.

In Modalità Cautela, il vostro computer risulta "nascosto" a software maligni e hacker. Il modulo Firewall è in grado di rilevare automaticamente e proteggere il computer contro i portscan (flusso di pacchetti spediti a una macchina per trovare "punti di accesso", spesso in preparazione di un attacco).

La sezione **Firewall** di questa guida all'utente comprende i seguenti punti:

- Approfondimenti Firewall
- Stato Firewall
- Protezione del Traffico
- Impostazioni Avanzate
- Attività Firewall
- Zone Rete

8.1. Approfondimento Firewall

Il Firewall BitDefender è stato progettato per offrire la miglior protezione alle vostre connessioni di rete / Internet, senza dover configurarlo. Non importa se siete connessi direttamente ad Internet, ad una singola rete oppure a diverse reti (Ethernet, wireless, VPN o altri tipi di rete), di fiducia o non di fiducia, il firewall si configurerà da solo per adattarsi alla situazione corrispondente.

Di default, BitDefender rileva automaticamente la configuarazione di rete del vostro computer e crea un appropriato profilo di base del firewall. Aggiunge anche al profilo le reti rilevate come zone di rete di fiducia o non fiducia a seconda della lor configurazione.

8.1.1. Cosa sono i Profili Firewall?

Un profilo firewall è un set di regole che controlla l'accesso delle applicazioni alla rete / Internet.

A seconda della configurazione di rete del vostro computer BitDefender crea automaticamente un tipo specifico di profilo. Il profilo di base creato contiene regole di accesso alla rete o regole elementari di accesso ad Internet, richieste dalle applicazioni del sistema e dalle componenti BitDefender.

Nota
Viene creato un singolo profilo firewall indipendentemente dal numero di reti a cui siete connessi.

Ci sono tre tipi di profili di base:

Profilo	Descrizione
Connessione Diretta	Contiene le regole elementari di accesso ad Internet consigliate per una configurazione di rete che permette l'accesso diretto ad Internet. Le regole non permettono agli utenti in rete di accedere al vostro computer nè a voi di sfogliare la rete.
Non di fiducia	Contiene le regole di accesso alla rete consigliate per una configurazione di rete associata a reti non di fiducia. Le regole vi permettono di sfogliare la rete ma impediscono ad altri utenti in rete di accedere al vostro computer.
Di fiducia	Contiene le regole di accesso alla rete consigliate per una configurazione di rete associata ad una rete di fiducia. Non si impongono restrizioni per l'accesso alla rete. Questo implica che voi avete accesso alle condivisioni in rete, stampanti di rete ed altre risorse di rete.Nell stesso tempo, i membri della rete possono connettersi al vostro computer ed accedere alle vostre condivisioni.

Man mano che le applicazioni cercano di collegarsi ad Internet, vengono aggiunte al profilo le regole appropriate. Potete scegliere di permettere o rifiutare per default l'accesso ad Internet delle applicazioni le cui regole non sono state ancora configurate oppure permettere per default solo alle applicazioni incluse nella White List e chiedere il permesso per le altre.

Nota

Per specificare le policy di accesso delle applicazioni che cercano di connettersi ad Internet per la prima volta, andare alla sezione Stato ed impostare il livello di protezione. Per modificare un profilo esistente, andare alla sezione Traffico e quindi cliccare su **Modificare Profilo Profile**.

8.1.2. Cosa sono le Zone Rete?

Una zona rete rappresenta un computer dentro ad una rete oppure un'intera rete completamente isolata dal vostro computer o, al contrario, una rete che può rilevare il vostro computer e connettersi ad esso. In pratica, una zona è un indirizzo IP o un range di indirizzi IP a cui è permesso o negato l'accesso al vostro computer.

Di default, BitDefender aggiunge automaticamente delle zone per specifiche configurazioni di rete. Una zona viene aggiunta al profilo corrente mediante la creazione di un'appropriata regola di accesso alla rete, applicabile ad un'intera rete.

Ci sono due tipi di zone:

Tipo di Zona	Descrizione
Di fiducia	I computer di una zona di fiducia possono connettersi al vostro computer e voi potete connettervi ai loro. Tutti i tentativi di connessione provenienti da una zona come questa, così come i tentativi di connessione dal vostro computer a questa zona sono autorizzati. Se una rete viene aggiunta ad una zona di fiducia, avrete accesso illimitato alle condivisioni di rete, stampanti di rete ed altre risorse di rete. Anche i membri della rete potranno connettersi al vostro computer ed accedere alle vostre condivisioni.
Non di fiducia	I computer da una zona non di fiducia non possono connettersi al vostro computer e neanche voi potete connettervi ai loro. Tutti i tentativi di connessione provenienti da una zona come questa, così come i tentativi di connessione dal vostro computer a questa zona sono bloccati. Siccome il traffico ICMP è bloccato e la Modalità Cautela è attiva, il vostro computer è praticamente invisibile ai computer di questa zona.

Nota

Per modificare una zona, andare alla sezione Zone. Per modificare una regola corrispondente ad una zona, andare alla sezione Traffico e cliccare **Modificare Profilo**.

8.1.3. Operazione Firewall

Quando si riavvia il sistema dopo l'installazione, BitDefender rileva automaticamente la vostra configurazione di rete, crea l'appropriato profilo di base ed aggiunge una zona a seconda della rete rilevata.

Nota

Se vi connettete direttamente ad Internet, nessuna zona verrà creata per la corrispondente configurazione di rete. Se siete connessi a più di una rete, le zone verrano aggiunte a seconda delle rispettive reti.

Ogni volta che la configurazione di rete cambia, perchè vi connettete ad un'altra rete o perchè disattivate una connessione di rete, viene creato un nuovo profilo firewall. Nello stesso tempo, le zone rete vengono modificate di conseguenza.

Quando si crea un nuovo profilo firewall, il vecchio profilo viene salvato, in modo che possa essere riutilizzato quando tornate alla sua configurazione di rete corrispondente.

A seconda della configurazione di rete, BitDefender si autoconfigurerà di conseguenza. Di default, Firewall BitDefender viene configurato così:

- Se vi connettete direttamente ad Internet, non importa se siete connessi ad altre reti, verrà creato un profilo Connessione Diretta. Altrimenti, BitDefender creerà un profilo firewall non di fiducia.

Nota

Per questione di sicurezza, i profili di ficudia non vengono creati di default. Per creare un profilo di fiducia, dovete azzerare il profilo esistente. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Reimpostare i Profili*» (p. 120).

- Le zone vengono aggiunte a seconda della configurazione di rete.

Tipo di Zona	Configurazione di rete
Di fiducia	**IP privato senza gateway** - Il computer fa parte di una rete locale (LAN) e non si connette ad Internet. Un esempio di questa situazione è una rete di casa creata per permettere

Tipo di Zona	Configurazione di rete
	ai membri della famiglia di condividere file, stampanti ed altre risorse.
	IP privato con Controllore di Dominio rilevato - Il computer fa parte di una LAN ed è connesso ad un dominio. Un esempio di questa situazione è una rete di ufficio creata per permettere agli utenti di condividere file ed altre risorse dentro un dominio. Un dominio implica l'esistenza di una serie di policies che i computer dei membri soddisfano.
Non di fiducia	**Wireless Aperta(non sicura)** - Il computer fa parte di una rete locale wireless (WLAN). Un esempio di questa situazione si verifica quando accedete ad Internet utilizzando un punto d'accesso libero da un luogo pubblico.

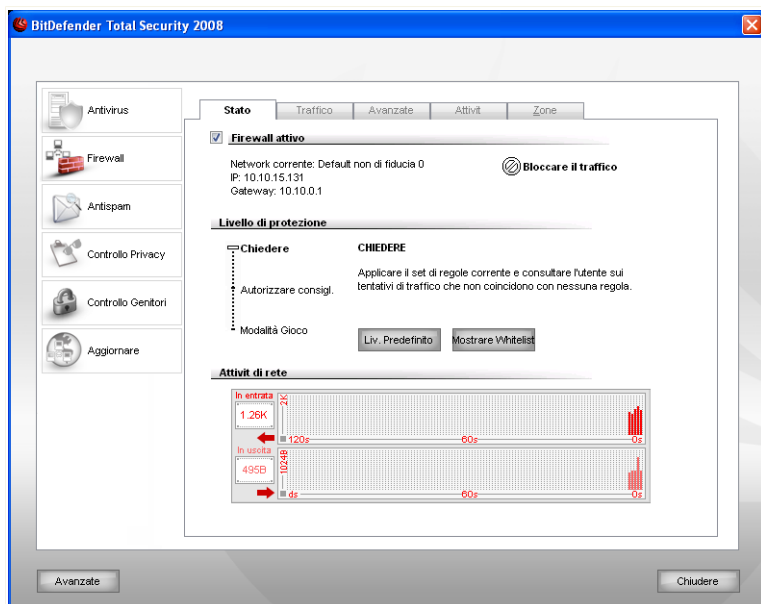
Nota

Le zone non vengono create per alcune configurazioni di rete come:

- **IP Pubblico (routable)** - Il computer è direttamente connesso ad Internet.
- **IP Privato con gateway, ma senza Controllore di Dominio rilevato** - Il computer fa parte di una LAN, senza fare parte di alcun dominio, e si connette ad Internet attraverso un gateway. Un esempio di questa situazione è una rete di un campus scolastico che permette agli utenti di condividere file ed altre risorse.

- Modalità Cautela (Stealth) è attiva.
- VPN e Connessione Remota sono permessi.
- Condivisione della Connessione ad Internet non è permessa per le zone non di fiducia.
- Si permette automaticamente l'accesso delle applicazioni incluse nella White List, mentre per le altre applicazioni vi verrà chiesto il permesso la prima volta che cercheranno di connettersi.

8.2. Stato del Firewall

Per configurare la protezione firewall, cliccare su **Firewall>Stato** nel console di configurazione. Apparirà la finestra seguente:

Stato del Firewall

In questa sezione potete abilitare/disabilitare il **Firewall**, bloccare tutto il traffico della rete/internet e configurare il comportamento predefinito sui nuovi eventi.

Importante
Per essere protetti contro gli attacchi via Internet, mantenere il **Firewall** abilitato.

Per bloccare tutto il traffico della rete/Internet, è sufficiente cliccare su **Blocca Traffico** e poi su **Sì** per confermare la vostra scelta. In questo modo isolerete il vostro computer da qualsiasi altro computer nella rete.

Per bloccare tutto il traffico più recente, cliccare semplicemente su **Sblocca Traffico**.

Nel lato inferiore della sezione potete vedere le statistiche BitDefender a proposito del traffico in arrivo e in uscita. Il grafico mostra il volume del traffico internet degli ultimi due minuti.

Nota
Il grafico appare anche se il **Firewall** è disabilitato.

8.2.1. Configurazione del Livello di Protezione

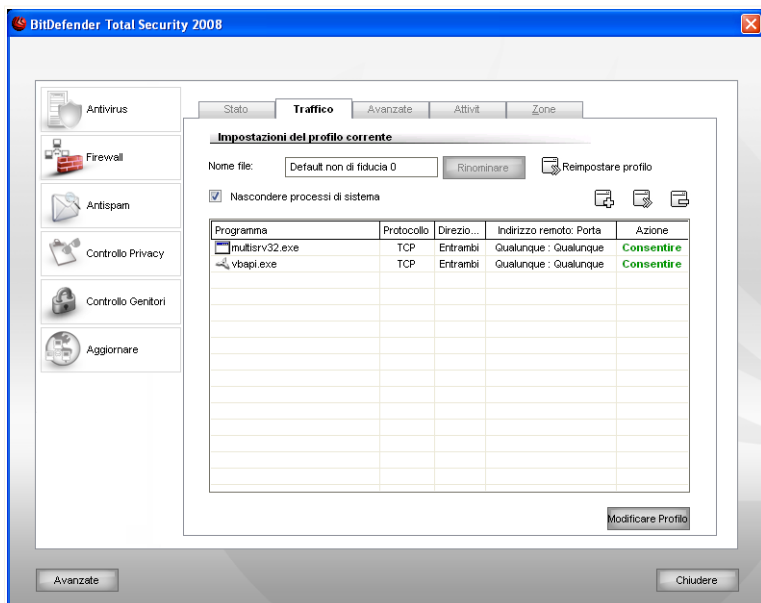
Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Modalità Gioco	Applica le regole correnti e permette tutti i tentativi di traffico che non corrispondono con le regole correnti senza chiedere il consenso. Questa policy è vivamente scondsigliata però potrebbe essere utile per amministratori di rete e giocatori (gamers).
Consentire consigliati	Applica le regole correnti e consente tutti i tentativi di connessione in uscita dai programmi conosciuti come legittimi (White List) da BitDefender senza chiedere il consenso. Per il resto dei tentativi di connessione, BitDefender vi chiederà il permesso. Potete vedere le regole di traffico così come sono create nella sezione Traffico. I programmi inclusi nella White List sono le applicazioni più comunemente utilizzate al mondo. Includono i browser più conosciuti, riproduttori audio;video, programmi di chat e condivisione file, così come applicazioni client server e di sistema operativo. Se volete vedere quali programmi sono nella White List, cliccare **Mostrare White List**.
Chiedere	Applica le regole correnti e chiede su tutti i tentativi di traffico chenon corrispondono ad una qualunque delle regole correnti di consenso.

Cliccare **Liv. Predefinito** per impostare la policy predefinita (**Consentire consigliati**).

8.3. Controllo del Traffico

Per gestire le regole di firewall del profilo corrente, cliccare su **Firewall>Traffico** nel console di configurazione. Apparirà la finestra seguente:

Controllo del Traffico

In questa sezione potete specificare quali connessioni in arrivo o uscita consentire o negare, creando regole con protocolli specifici, porte, applicazioni e/o indirizzi remoti.

Le regole possono essere immesse automaticamente (attraverso la finestra di avviso) oppure manualmente (selezionando **Aggiungere** e scegliendo i parametri per la la regola).

8.3.1. Aggiungere Regole Automaticamente

Con il **Firewall** abilitato, BitDefender chiederà il vostro consenso ogni volta che viene eseguita una connessione a Internet:

Avvisi del Firewall

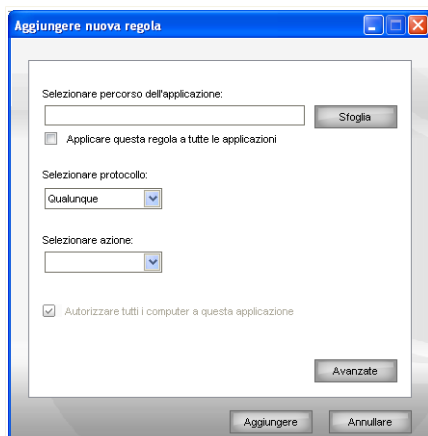
Potete vedere quanto segue: l'applicazione che sta provando ad accedere ad Internet, il percorso per il file dell'applicazione, la destinazione, il protocollo utilizzato e la porta sulla quale l'applicazione sta provando a connettersi.

Cliccare **Consentire** per permettere tutto il traffico (in entrata ed in uscita) generato da questa applicazione dall'host locale verso qualsiasi destinazione, attraverso il rispettivo protocollo IP e su tutte le porte. Se cliccate su **Bloccare**, all'applicazione verrà completamente negato l'accesso ad Internet attraverso il rispettivo protocollo IP.

Basandosi sulla vostra risposta, una regola verrà creata, applicata ed inserita nella tabella. La prossima voltra che l'applicazione cercherà di connettersi, quest aregola verrà applicata di default.

Importante
Consentire tentativi di connessioni in ingresso solo da IP o domini dei quali vi fidate.

8.3.2. Aggiungere Regole Manualmente

Selezionare **Aggiungi Regola** e scegliere i parametri. Apparirà la finestra seguente:

Aggiungere Regola

Per aggiungere una nuova regola firewall, seguire questi passaggi:

1. Selezionare l'applicazione per la quale la nuova regola di firewall verrà creata.

   Per selezionare un'applicazione, cliccare **Sfoglia**, localizzatela e quindi cliccare **OK**.

   Se volete creare una regola per tutte le applicazioni, selezionate semplicemente **Applicare questa regola a tutte le applicazioni**.
2. Selezionare il protocollo sul quale la regola verrà applicata.

   E' disponibile una lista con i protocolli più comuni, per aiutarvi a selezionarne uno specifico. Selezionare il protocollo desiderato (sul quale si applica la regola) dal corrispondente menu a tendina o selezionare **Qualsiasi** per tutti i protocolli.

   La seguente tabella elenca i protocolli tra i quali potete scegliere, con una breve descrizione di ognuno:

Protocollo	*Descrizione*
ICMP	Internet Control Message Protocol – è una estensione a Internet Protocol (IP). ICMP supporta pacchetti contenenti errori, controlli, e messaggi di informazione. Il comando PING, ad esempio, utilizza ICMP per testare una connessione Internet.

Protocollo	Descrizione
TCP	Transmission Control Protocol – Il Protocollo TCP abilita due host a stabilire una connessione e a scambiarsi pacchetti di dati. TCP garantisce la consegna dei dati e anche le garanzie che questi pacchetti saranno consegnati nello stesso ordine in cui sono stati inviati.
UDP	User Datagram Protocol – UDP è un IP progettato per elevate prestazioni. I giochi e altre applicazioni video utilizzano spesso UDP.

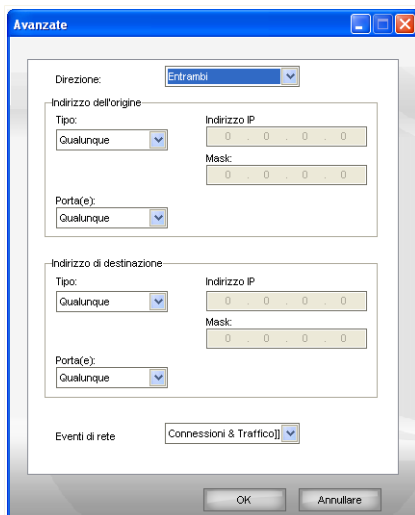
3. Selezionare l'azione della regola dal menu corrispondente.

Azione	Descrizione
Consenti	L'accesso alla rete / Internet dell'applicazione verrà autorizzato quando si verifichino le circostanze specificate.
Impedisci	L'accesso alla rete / Internet dell'applicazione verrà negato le circostanze specificate.

4. Se il protocollo selezionato in precedenza è TCP o UDP, potrete specificare se la regola verrà applicata o meno all'applicazione quando questa funziona come server.

   Selezionare **Consentire ad altri computer di connettersi a questa applicazione** per applicare l'azione a tutti gli eventi di rete. Implicitamente, consentirete o negherete il diritto di questa applicazione ad aprire le porte.

   Se volete applicare l'azione solo al traffico UDP oppure solo al traffico TCP, deselezionare le caselle corrispondenti.

Se volete configurare ulteriori impostazioni avanzate per la regola, cliccare su **Avanzate**. Una nuova finestra apparirà:

Impostazioni Avanzate della Regola

E' possibile configurare quanto segue:

- **Direzione** - seleziona la direzione del traffico.

Tipo	Descrizione
In Uscita	La regola è applicata solo al traffico in uscita.
In Entrata	La regola è applicata solo al traffico in entrata.
Entrambe	La regola sarà applicata in entrambe le direzioni.

- **Indirizzo di Origine** - specificare l'indirizzo della fonte.

  Per specificare l'indirizzo di origine, selezionare il tipo d'indirizzo dal menu e quindi specificare i dati richiesti. Sono disponibili le seguenti opzioni:

Tipo	Descrizione
Qualsiasi	La regola verrà applicata a tutti gli indirizzi di origine.

Tipo	Descrizione
Host	La regola viene applicata solo se l'origine è un host specifico. Dovete inserire l'indirizzo IP del host.
Rete	La regola viene applicata solo se l'origine è una rete specifica. Dovete inserire l'indirizzo IP e la maschera di rete.
Host Locale	La regola viene applicata solo se l'origine è il host locale. Se utilizzate più di un interfaccia di rete, selezionare dal menu l'interfaccia di rete al quale la regola verrà applicata. Se volete che la regola venga applicata a tutti gli host locali, selezionare **Qualsiasi**.
Rete Locale	La regola viene applicata solo se l'origine è una rete locale. Se siete connessi a più di una rete, selezionare dal menu la rete alla quale la regola verrà applicata. Se volete che la regola venga applicata a tutte le reti locali, selezionare **Qualsiasi**.

Se avete selezionato TCP o UDP come protocollo, potete impostare una porta specifica oppure un range tra 0 e 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.

- **Indirizzo Destinazione** - specificare l'indirizzo di destinazione.

Per specificare l'indirizzo della destinazione, selezionare il tipo di indirizzo dal menu e specificare i dati richiesti. Sono disponibili le seguenti opzioni:

Tipo	Descrizione
Qualsiasi	La regola verrà applicata a qualsiasi indirizzo di destinazione.
Host	La regola verrà applicata solo se la destinazione è un host specifico. Dovete inserire l'indirizzo IP del host.
Rete	La regola verrà applicata solo se la destinazione è una rete specifica. Dovete inserire l'indirizzo IP e la maschera di rete.
Host Locale	La regola verrà applicata solo se la destinazione è l'host locale. Se utilizzate più di un interfaccia di rete, selezionare dal menu l'interfaccia di rete al quale la regola verrà applicata. Se volete che la regola venga applicata a tutti gli host locali, selezionare **Qualsiasi**.

Tipo	Descrizione
Rete Locale	La regola verrà applicata solo se la destinazione è la rete locale. Se siete connessi a più di una rete, selezionare dal menu la rete alla quale la regola verrà applicata. Se volete che la regola venga applicata a tutte le reti locali, selezionare **Qualsiasi**.

Se avete selezionato TCP o UDP come protocollo, potete impostare una porta specifica oppure un range tra 0 e 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.

- **Eventi di Rete** - se avete selezionato TCP o UDP come protocollo, scegliere gli eventi di rete sui quali applicare la regola.

Selezionare **OK** per chiudere la finestra delle impostazioni avanzate.

Cliccare su **Aggiungi** per aggiungere la regola firewall.

8.3.3. Amministrazione delle regole

Nella tabella potete vedere l'elenco delle regole create finora per il profilo corrente.

Selezionare la casella di controllo corrispondente a **Nascondere i processi di sistema** per nascondere le regole riguardanti i processi di sistema o BitDefender.

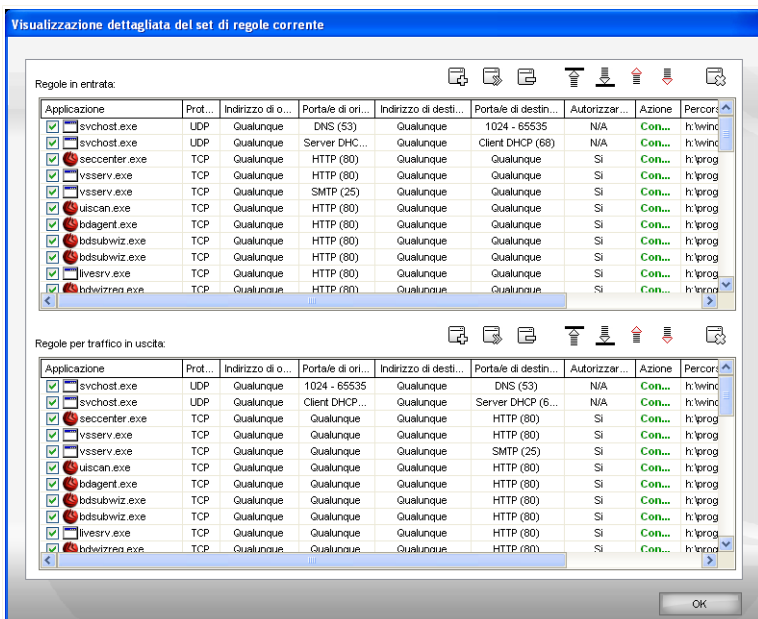
Le regole sono elencate in ordine di importanza partendo dalla prima, che ha la priorità più alta. Per modificare la priorità delle regole, spostandole in alto o in basso, selezionare **Edita profilo** per visualizzare **Vista Dettagliata** dove eseguire le modifiche.

Per cancellare una regola, selezionarla e cliccare sul tasto **Eliminare regola**.

Per editare una regola, selezionarla e cliccare sul tasto **Modificare regola** oppure fare un doppio click.

Nota
E' inoltre disponibile un menu contestuale che contiene le seguenti opzioni: **Aggiungi Regola**, **Elimina Regola** e **Edita Regola**.

8.3.4. Modifica dei Profili

Potete modificare un profilo facendo un click su **Editare profilo**. Comparirà la seguente finestra:

Vista Dettagliata

Le regole sono divise in 2 sezioni: regole in entrata e regole in uscita. Potete vedere l'applicazione e i parametri delle regole di ciascuna regola (indirizzo origine, indirizzo destinatario, porte origine, porte di destinazione, azione, ecc).

Per cancellare una regola è sufficiente selezionarla e cliccare sul tasto **Eliminare Regola**. Per cancellare tutte le regole cliccare sul tasto **Cancellare Elenco**. Per modificare una regola, selezionarla e cliccare sul tasto **Modificare Regola** oppure eseguire un doppio click su questa. Per disattivare temporaneamente una regola senza cancellarla, deselezionare la casella corrispondente.

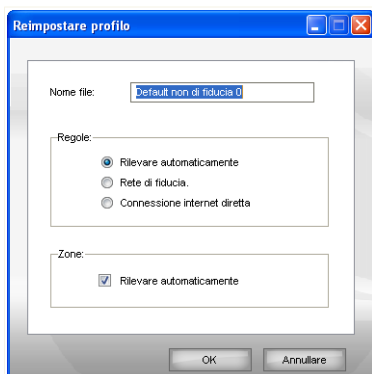
Potete alzare o abbassare la priorità di una regola. Fare un clck sul bottone **Sposta in alto** per alzare la priorità della regola selezionata di un livello, oppure fare un click sul bottone **Sposta in basso** per abbassare la priorità della regola selezionata, di un livello. Per assegnare ad una regola la massima priorità cliccare sul tasto **Spostare all'inizio**. Per assegnare ad una regola la minima priorità cliccare sul tasto **Spostare alla fine**.

Nota

E' inoltre disponibile un menu contestuale che contiene le seguenti opzioni: **Aggiungere Regola**, **Modificare Regola**, **Eliminare Regola**, **Spostare in alto**, **Spostare in basso**, **Spostare all'inizio**, **Spostare alla fine** e **Cancellare Elenco**.

Selezionare **OK** per chiudere la finestra.

8.3.5. Reimpostare i Profili

Gli utenti avanzati possono scegliere di riconfigurare il profilo firewall per ottimizzare la protezione firewall oppure per personalizzarlo d'accordo con le proprie necessità. Per reimpostare il profilo firewall, cliccare su **Reimpostare Profilo**. Apparirà la finestra seguente:

Reimpostazione del profilo

E' possibile configurare quanto segue:

- **Nome Profilo** - inserire un nuovo nome nel campo di modifica.
- **Regole** - specificare che tipo di regole dovrebbero essere create per le applicazioni del sistema.

  Sono disponibili le seguenti opzioni:

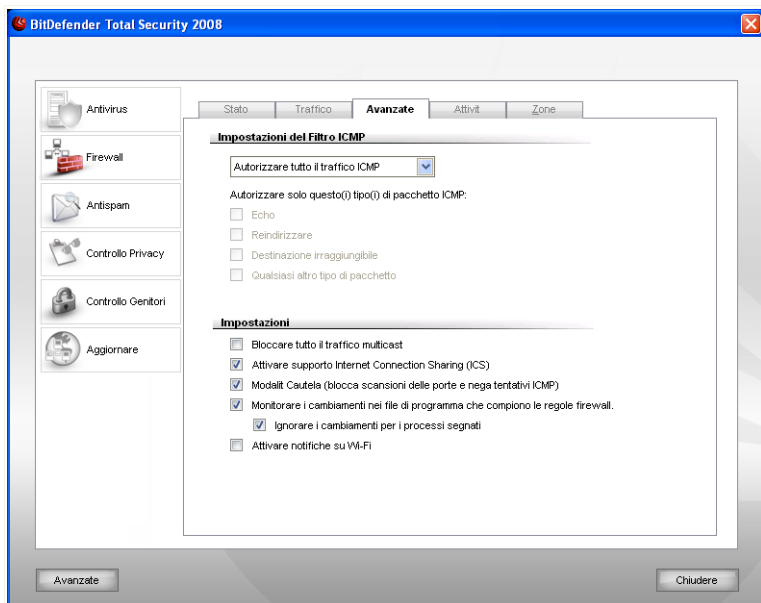
Opzione	*Descrizione*
Auto-rilevamento	Permette a BitDefender di rilevare la configurazione di rete e di creare un set appropriato di regole elementari.
Rete di fiducia	Crea un set di regole elemantari appropriato per una rete di fiducia.
Connessione diretta ad Inernet	Crea un set di regole elemantari appropriato per una connessione diretta ad Inernet.

- **Zone** - selezionare **Auto-rilevamento** per permettere a BitDefender di creare delle zone appropriate per le reti rilevate.

Selezionare **OK** per chiudere la finestra e reimpostare il profilo.

Importante
Tutte le regole che avete aggiunto in questa sezione andranno perse se scegliete di riconfigurare il profilo di firewall.

8.4. Impostazioni Avanzate

Per configurare le impostazioni avanzate del firewall BitDefender, cliccare su **Firewall>Avanzate** nel console di configurazione. Apparirà la finestra seguente:

Impostazioni Avanzate

In questa sezione potete configurare le impostazioni avanzate del firewall BitDefender. Le impostazioni avanzate vi consentono di specificare le regole di filtraggio per il traffico ICMP (Impostazioni Filtro ICMP) e di bloccare il traffico a trasmissioni multiple, di sondividere la vostra connessione Internet o di rendere il vsotro computer invisibile a software maligno e a hacker (Settings).

8.4.1. Configurazione delle Impostazioni dei Filtri ICMP

Dal menu, potete selezionare una delle seguenti politiche per filtrare il traffico ICMP:

- **Consentire tutto il traffico ICMP** - consente tutto il traffico ICMP.
- **Bloccare tutto il traffico ICMP** - blocca tutto il traffico ICMP.
- **Personalizzare Filtro ICMP** personalizza il modo in cui il traffico ICMP viene filtrato. Sarete in grado di scegliere i tipi di pacchetti ICMP da consentire.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Echo	Questa opzione consente l'Echo Replay e i messaggi Echo Request. L'Echo Requeset è un messaggio ICMP che invia un pacchetto di dati all'host e si aspetta che questi dati siano rispediti in un Echo Replay. L'host deve rispondere a tutti gli Echo Requests con un Echo Replay contenente i dati esatti, ricevuti nel messaggio request. L'Echo Replay è un messaggio ICMP generato in risposta al messaggio ICMP Echo Request, ed è obbligatorio per tutti gli hosts e routers.
Redirect	Questo è un messaggio ICMP che informa un host, per indirizzare le sue informazioni routing (a inviare pacchetti su una via alternativa). Se l'host prova a inviare dati attraverso un router (R1) e quindi un altro router (R2) per raggiungere l'host e un percorso diretto dall'host a R2 è valido, una nuova direzione vi informerà l'host di tale route. Il router invierà ancora il datagram originale alla destinazione destinata. Tuttavia, se il datagram contiene informazioni routing, questo messaggio non sarà inviato , anche se è disponibile un'instadamento migliore.
Destinazione Irraggiungibile	Questo è un messaggio ICMP generato dal router per informare il client che l'host di destinazione è irraggiungibile, a meno che il datagram non abbia un indirizzo a diffusione multipla. Tra le ragioni che provocano il messaggio vi sono la mancanza del collegamento fisico all'host (la distanza è infinita), il protocollo o la porta indicata non sono attivi, o i dati devono essere frammentati ma l'indicatore " non frammentate" è attivo.
Qualsiasi altro tipo di pacchetto	Con questa opzione abilitata , qualsiasi altro pacchetto di **Echo**, **Destinazione Irraggiungibile** o **Reindirizzazione**passerà.

- **Applicare il set di regole corrente per ICMP** - applica al traffico ICMP le impostazioni correnti stabilite nella sezione Stato del modulo **Firewall**.

8.4.2. Configurazione delle Impostazioni Avanzate Firewall

Sono disponibili le seguenti impostazioni avanzate del firewall:

- **Bloccare tutto il traffico multicast** - rilascia qualsiasi pacchetto multicast ricevuto.

  Il traffico Multicast è il tipo di traffico che si indirizza ad un gruppo particolare in una rete. I pacchetti sono inviati ad indirizzi speciali da cui il client multicast può riceverli se accetta di farlo.

  Ad esempio, un membro di una rete che possiede un sintonizzatore TV può trasmettere (inviare ad ogni membro della rete) o inviare in multicast (inviare ad un indirizzo speciale) il flusso video. I computer che ascoltano l'indirizzo multicast possono accettare o rifiutare il pacchetto. Se accettato, il flusso video può essere visto dai client multicast.

  Quantità eccessive di traffico multicast consumano banda e risorse. Con questa opzione abilitata qualsiasi pacchetto multicast ricevuto sarà rilasciato. Comunque, non si raccomanda di selezionare questa opzione.
- **Abilita il supporto Condivisione Connessione Internet(ICS)** - abilita il supporto per la Condivisione Connessione Internet (ICS).

  Nota
  Questa opzione non abilita automaticamente ICS sul vostro sistema, ma consente solo questo tipo di connessione nel caso voi la abilitiate dal vostro sistema operativo.

  La Condivisione della Connessione Internet (ICS) permette ai membri delle reti locali di collegarsi ad Internet attraverso il vostro computer. Ciò è utile quando usufruite di una connessione Internet speciale/particolare (es. connessione wireless) e volete condividerla con altri membri della vostra rete.

  Condividere la vostra connessione Internet con i membri delle reti locali porta ad un livello di consumo risorse più alto e può comportare un certo rischio. Taglia anche alcune delle vostre porte (quelle aperte dai membri che stanno utilizzando la vostra connessione Internet).
- **Modalità Invisibile** - rende invisibile il vostro computer al software maligno e agli hacker.

  Un modo semplice di scoprire se il vostro computer può essere vulnerabile è collegarsi alle porte per vedere se vi è risposta. Ciò è chiamato portscan.

  Individui malintenzionati o programmi software, non devono conoscere l’esistenza del vostro computer e tanto meno fornire servizi alla rete. L’opzione **Modalità**

Invisibile impedirà alla vostra macchina di rispondere ai tentativi di scoprire quali porte sono aperte o dove sia esattamente nella rete.

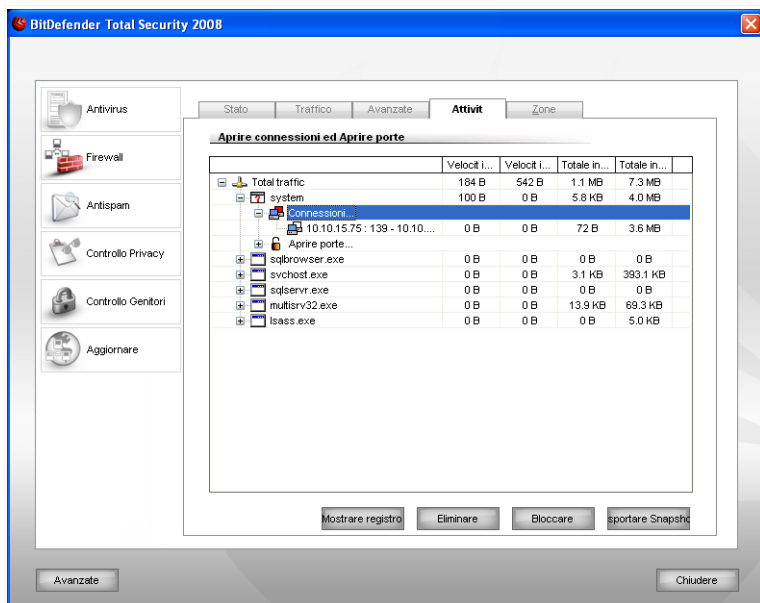
- **Monitorare le modifiche dei file di programma corrispondenti con le regole del firewall** - esamina ogni applicazione che tenta di connettersi ad Internet per vedere se è cambiata da quando è stata aggiunta la regola che controlla il suo accesso. Se l'applicazione è stata modificata, un avviso vi chiederà di consentire o di bloccare l'accesso dell'applicazione ad Internet.

  Normalmente, le applicazioni vengono modificate dagli aggiornamenti. Ma c'è il rischio che vengano modificate da applicazioni malware, con il proposito di infettare il vostro computer ed altri computer in rete.

  Nota
  Vi consigliamo di mantenere attiva questa opzione e di consentire l'accesso solo alle applicazioni che vi aspettate vengano modificate dopo che la regola di controllo del loro accesso è stata creata.

  Le applicazioni segnalate si suppone che siano di fiducia e che abbiano un più alto grado di sicurezza. Potete selezionare **Ignorare le modifiche per i processi segnalati** per consentire alle applicazioni segnalate che siano cambiate, di connettersi ad Internet senza che riceviate un avviso di questo evento.
- **Attivare notifiche di Wi-Fi** - attiva le notifiche di Wi-Fi.

8.5. Controllo Connessione

Per monitorare l'attività della rete/internet corrente (su TCP e UDP) generata dall' applicazione ed aprire il registro del Firewall BitDefender, cliccare su **Firewall>Attività** nel console di configurazione. Apparirà la finestra seguente:

Controllo Connessione

E' possibile visualizzare il traffico totale generato dall'applicazione. Per ogni applicazione, è possibile visualizzare le connessioni e le porte aperte, così come le statistiche riguardanti la velocità del traffico in uscita ed in entrata e la quantità totale di dati inviati / ricevuti.

La finestra presenta l'attività della rete corrente / Internet in tempo reale. Se le connessioni o le porte fossero chiuse, potreste vedere che le statistiche corrispondenti sarebbero opache e che, alla fine, scomparirebbero. La stessa cosa accade a tutte le statistiche corrispondenti ad un'applicazione che genera traffico o ha delle porte aperte e che voi chiudete.

Per creare regole che limitano il traffico dell'applicazione selezionata, porta o connessione, fare un click su **Blocca**. Vi sarà richiesto di confermare la vostra scelta. Si può accedere alla regola, per una ulteriore "messa a punto", nella sezione Traffico.

Fare un click su **Export Snapshot** per esportare la lista in un file `.txt`.

Per una lista completa degli eventi riguardanti l'uso del modulo Firewall (avvio/arresto firewall, blocco del traffico, attivazione Modalità Cautela, modifica delle impostazioni,

applicazione di un profilo) o generati dalle attività da esso rilevate (scansione porte, blocco tentativi di connessione o del traffico secondo le regole), controllare il file di registro del Firewall BitDefender, il quale può essere visualizzato cliccando su **Mostrare Registro**. Il file si trova nella cartella File Comuni dell'utente corrente Windows, sotto il percorso: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

8.6. Zone di rete

Una zona è un indirizzo IP o un range di indirizzi Ip per i quali è stata creata una regola speciale dentro un profilo. La regola può consentire ai membri della rete un accesso illimitato al vostro computer (zone di fiducia) o, al contrario, isolare completamente il vostro computer dai computer in rete (zone non di fiducia).

Di default, BitDefender rileva automaticamente la rete alla quale siete connessi ed aggiunge una zona a seconda della configurazione di rete.

Nota
Se siete connessi a diverse reti, a seconda della loro configurazione, può essere aggiunta più di una zona.

Le zone di fiducia vengono aggiunte di default per le seguenti configurazioni di rete:

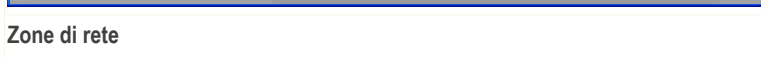
- **IP Privato senza gateway** - Il computer fa parte di una rete locale (LAN) e non si connette ad Internet.
- **IP privato con Controllore di Dominio rilevato** - Il computer fa parte di una LAN ed è connesso ad un dominio.

Le zone non di fiducia vengono aggiunte di default per le seguenti configurazioni di rete:

- **Wireless Aperta(non sicura)** - Il computer fa parte di una rete locale wireless (WLAN).

Per gestire le zone di rete cliccare su **Firewall>Zone** nel console di configurazione. Apparirà la finestra seguente:

Zone di rete

Nella tabella potete vedere l'elenco delle zone di rete corrispondenti al profilo corrente. per ogni zona potete vedere il tipo di rete (Ethernet, wireless, PPP ed altri), il computer o la rete associati a quella zona e se la zona è o non è di fiducia.

Per modificare una zona, selezionarla e cliccare sul tasto **Modificare Zona** o cliccarci due volte.

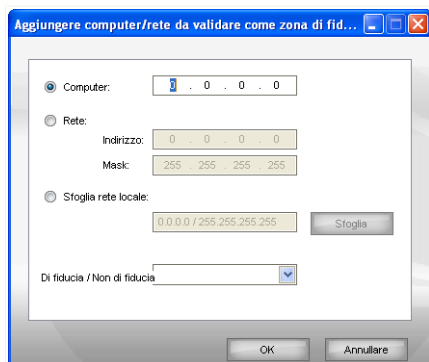
Nota

Di default, BitDefender aggiunge le reti wireless aperte come zone non di fiducia. Se siete connessi ad una rete wireless aperta ad-hoc con dei computer di fiducia (a casa o con un paio di amici), potreste voler modificare la zona associata. Per essere in grado di condividere delle risorse con gli altri membri della rete, dovete impostare la rete come zona di fiducia.

Per eliminare una zona , selezionarla e cliccare sul tasto **Eliminare Zona**.

8.6.1. Aggiungere Zone

E' possibile aggiungere zone manualmente. Questo vi permette, per esempio, di condividere file solo con i vostri amici dentro una rete wireless aperta (aggiungendo questi computer come zone di fiducia), oppure di bloccare un computer di una zona di fiducia (aggiungendolo come zona non di fiducia).

Per aggiungere una nuova zona, cliccare sul tasto **Aggiungere Zona**. Apparirà la finestra seguente:

Aggiungere Zona

Per aggiungere una zona, seguire questi passaggi:

1. Specificare un computer da una rete locale o un'intera rete locale che volete venga aggiunto come una zona. Potete usare uno dei metodi seguenti:
   - Per aggiungere un computer specifico, selezionare **Computer** e fornire l'indirizzo IP.
   - Per aggiungere una rete specifica, selezionare **Reter** e fornire l'indirizzo IP e maschera.
   - Sfogliare le reti locali per trovare ed aggiungere un computer od una rete.

     Per sfogliare le reti locali, selezionare **Sfogliare rete locale** e poi cliccare su **Sfoglia**. Apparirà una nuova finestra dove potrete vedere tutte le reti alle quali siete connessi così come tutti i membri di ogni rete.

     Selezionare dalla lista il computer o la rete che volete aggiungere come zona e cliccare **OK**
2. Selezionare dal menu che tipo di zona volete creare (di fiducia o non di fiducia).

3. Cliccare **OK** per aggiungere la zona.

9. Antispam

Antispam BitDefender impiega notevoli innovazioni tecnologiche e filtri standard dell'industria antispam per eliminare lo spam prima che raggiunga l'Inbox dell'utente.

La sezione **Antispam** di questa guida all'utente comprende i seguenti argomenti:

- Approfondimenti Antispam
- Stato Antispam
- Impostazioni Antispam
- Integrazione nei client di posta

9.1. Approfondimenti Antispam

Lo Spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Non è piacevole, vorreste evitare che i vostri figli lo vedessero, potrebbe penalizzarvi (per aver sprecato troppo tempo o per aver ricevuto mail pornografiche in ufficio) e non potete impedire ad alcuni di inviarlo. La miglior cosa da fare, ovviamente, e di bloccare la ricezione. Purtroppo lo Spam si presenta sotto molte forme e dimensioni e ce n'è tantissimo.

9.1.1. Filtri Antispam

Il Motore Antispam BitDefender incorpora sette diversi filtri che assicurano l'assenza di SPAM nella vostra Inbox: White list, Black list, Filtro Carattere, Filtro Immagine, Filtro URL, Filtro Heuristico e Filtro Bayesiano.

Nota
E' possibile attivare/disattivare ognuno di questi filtri nel modulo **Antispam**, sezione Impostazioni.

White List / Black List

La maggior parte delle persone comunica regolarmente con un gruppo di persone o riceve messaggi da organizzazioni o società nello stesso dominio. Utilizzando **L'elenco Amici o Spammer**, potrete facilmente classificare da quali persone volete ricevere e-mail (Amici) indipendentemente dal contenuto del messaggio, o da quali persone non volete più ricevere nulla (spammer).

Nota
White list / Black list sono anche conosciute come corrispondenti a **Elenco Amici / Elenco Spammer**.

E’ possibile gestire **l’elenco Amici/Spammer** dalla Console di Configurazione oppure dalla barra strumenti Antispam integrata in alcuni dei più comunemente usati client di posta.

Nota
Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all’**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell’elenco; inoltre aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Filtro Carattere

La maggior parte dei messaggi Spam sono scritti in caratteri cirillici e/o asiatici. Il filtro Carattere rileva questo tipo di messaggi e li etichetta come SPAM.

Filtro Immagine

Da quando la detenzione heuristica è diventata una realtà, le cartelle di posta in arrivo sono piene di molti messaggi contenenti solo una immagine con contenuti insoliti. Per contrastare questo problema, BitDefender ha introdotto il **Filtro Immagine** che confronta le impronte delle immagini contenute nelle e-mail con il proprio database. In caso di riconoscimento, la e-mail sarà etichettata come Spam.

Filtro URL

La maggior parte dei messaggi Spam contiene links a vari siti web. Questi siti solitamente contengono ulteriore pubblicità e la possibilità di acquistare oggetti e, alle volte, vengono usati per phishing.

BitDefender mantiene un database di tali links. Il filtro URL esamina ogni link URL contenuto in un messaggio con il suo database. Se corrisponde, il messaggio viene etichettato come SPAM.

Filtro Euristico

Il **Filtro Euristico** esegue una serie di tests a tutte le componenti del messaggio (ovvero, non solo l’intestazione ma anche il corpo del messaggio sia in formato HTML che di testo), alla ricerca di parole, frasi, links o altri elementi caratteristici dello SPAM. Basandosi sui risultati dell'analisi, esso aggiunge un punteggio SPAM al messaggio.

Il filtro rileva inoltre messaggi segnati come `ESPLICITAMENTE SESSUALE:` nell'oggetto e li etichetta come SPAM.

Nota
A partire dal 19 Maggio 2004 lo Spam contenente materiale a sfondo sessuale deve includere l'avviso `SEXUALLY-EXPLICIT` nell'oggetto, diversamente sarà passibile di sanzioni per violazione della legge federale.

Filtro Bayesiano

Il modulo **Filtro Bayesiano** classifica i messaggi secondo informazioni statistiche relative alla frequenza di specifiche parole, contenute nei messaggi classificati come Spam in comparati a quelli dichiarati come non-SPAM (da voi o dal filtro euristico).

Ciò significa, ad esempio, che se una determinata parola di quattro lettere appare più spesso in uno Spam, è naturale desumere che esiste una notevole possibilità che il successivo messaggio in entrata, contenente la stessa parola, SIA SPAM. Vengono prese in considerazione tutte le parole rilevanti all'interno di un messaggio. Sintetizzando le informazioni statistiche, viene valutata la probabilità che l'intero messaggio sia SPAM.

Questo modulo presenta un'altra interessante caratteristica: lo si può "formare", istruire. Si adegua rapidamente al tipo di messaggi ricevuti da un determinato utente e immagazzina informazioni su tutto. Per funzionare efficacemente, il filtro deve essere "istruito", ovvero gli vanno presentati esempi di SPAM e di messaggi leciti, proprio come si addestra un cane da caccia a rilevare determinati odori. A volte il filtro deve essere anche corretto – indotto a regolarsi quando prende una decisione sbagliata.

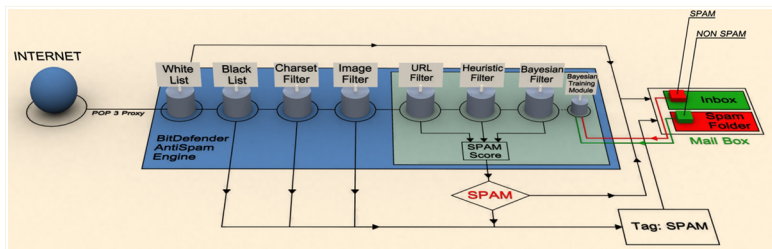
Importante
E' possibile correggere il modulo Bayesiano utilizzando dalla Barra degli strumenti Antispam i pulsanti **E' Spam** e **Non è Spam**.

Nota
Ogni volta che eseguite un aggiornamento:

- nuove impronte di immagini saranno aggiunte al **Filtro Immagine**.
- nuovi links verranno aggiunti al **Filtro URL**.
- nuove regole verranno aggiunte al **Filtro Euristico**.

Questo aiuterà ad incrementare l'efficacia del vostro motore Antispam.
Per proteggervi contro gli spammers, BitDefender può effettuare aggiornamenti automatici. Mantenere l'opzione di **Aggiornamento Automatico** attivata.

9.1.2. Operazione Antispam

Lo schema mostra come funziona BitDefender.

Operazione Antispam

Il filtro Antispam dallo schema sopra (White list, Black list, Filtro Carattere, Filtro Immagine, Filtro URL , Filtro Heuristico e Filtro Bayesiano) sono utilizzati congiuntamente dal modulo Antispam di BitDefender per verificare se una determinata parte di mail deve essere inoltrata o no alla vostra **Inbox**.

Ogni e-mail che arriva da Internet viene prima controllata con la White list/Black list. Se l'indirizzo del mittente viene trovato nella White list l'e-mail viene spostata direttamente nella vostra **Inbox**.

Diversamente, il filtro Black list prenderà in carico l'e-mail per verificare se l'indirizzo del mittente è contenuto nel suo elenco. L'e-mail verrà marcata come SPAM e spostata nella cartella **Spam** (situata in Microsoft Outlook) qualora il confronto con la lista abbia dato esito positivo.

Ancora, il Filtro Carattere controllerà se l'e-mail è scritta con caratteri cirillici o asiatici. In questo caso l'e-mail verrà marcata come SPAM e spostata nella cartella **Spam**.

Qualora l'e-mail non fosse scritta con caratteri asiatici o cirillici, la stessa verrà passata al filtro Filtro Immagine. Il **Filtro Immagine** controllerà tutti i messaggi e-mail contenenti allegati con immagini con contenuti di spam.

Il Filtro URL cercherà i link e li comparerà con quelli del database di BitDefender. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

Il Filtro Euristico prenderà in carico l'e-mail ed eseguirà una serie di test su tutte le componenti del messaggio, alla ricerca di parole, frasi, collegamenti o caratteristiche dello Spam. Il risultato sarà quello di aggiungere un altro punteggio Spam alla e-mail.

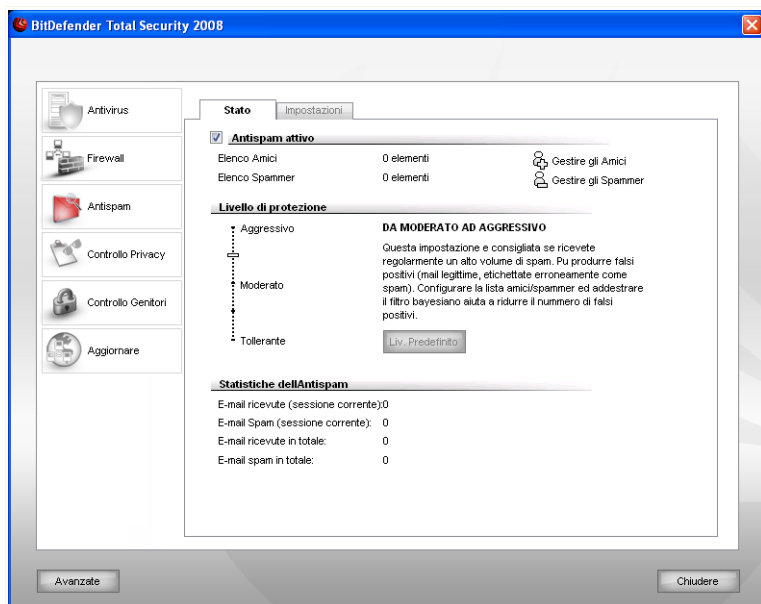
Nota
Se l'e-mail è marcata come SEXUALLY EXPLICIT nella riga del soggetto, BitDefender la considererà come SPAM.

Il modulo del Filtro Bayesiano analizzerà ulteriormente il messaggio, basandosi su informazioni statistiche relative all'incidenza con cui determinate parole appaiono nei messaggi classificati come Spam, in paragone a quelli dichiarati come non-Spam (da voi o dal filtro euristico). Verrà aggiunto un punteggio Spam alla e-mail.

Se il risultato del punteggio (punteggio URL + punteggio Euristico + punteggio Bayesiano) eccede il punteggio Spam per un messaggio (impostato dall'utente nella sezione Antispam come livello di tolleranza), il messaggio viene considerato come SPAM.

Importante
Se utilizzate un client di e-mail diverso da Microsoft Outlook o Microsoft Outlook Express, dovrete create una regola per spostare i messaggi e-mail contrassegnati come Spam da BitDefender in una cartella personalizzata di quarantena. BitDefender allega il prefisso `[SPAM]` al soggetto dei messaggi considerati come Spam.

9.2. Stato Antispam

Per configurare la protezione Antispam, cliccare su **Antispam>Stato** nel console di configurazione. Apparirà la finestra seguente:

Stato Antispam

In questa sezione potete configurare il modulo **Antispam** e visionare le informazioni relative alla sua attività.

Importante

Per impedire che lo Spam entri nella vostra **Inbox**, mantenere abilitato il **Filtro Antispam**.

Nella sezione **Statistiche** è possibile visionare i risultati della attivita dell' Antispam presentati per sessione (da quando avete avviato il vostro compiuter), oppure un riassunto (dalla installazione del BitDefender).

Per configurare il modulo **Antispam** è necessario procedere come segue:

9.2.1. Passaggio 1/2 - Impostazione del Livello di Tolleranza

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 5 livelli di tolleranza:

Livello di tolleranza	*Descrizione*
Tollerante	Offre protezione per gli account che ricevono molta posta commerciale legittima. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Tra Tollerante e Moderato	Offre protezione per account che ricevono alcune mail commerciali legittime. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Moderata	Offre protezione per account normali. Il filtro bloccherà la maggior parte dello spam, evitando al contempo i falsi positivi.
Da Moderata ad Aggressiva	Offre protezione per gli account che ricevono regolarmente ampi volumi di spam. Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Configura gli **Elenchi Amici/Spammer** e addestra il **Motore di Apprendimento (Bayesiano)** per ridurre il numero di falsi positivi.
Aggressiva	Offre protezione per gli account che ricevono regolarmente volumi di spam molto ampi. Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Aggiungete i vostri contatti alla **Lista Amici** per ridurre il numero di falsi positivi.

Per impostare il livello di protezine di default (**Da Moderata ad Aggressiva**) cliccare su **Livello di Default**.

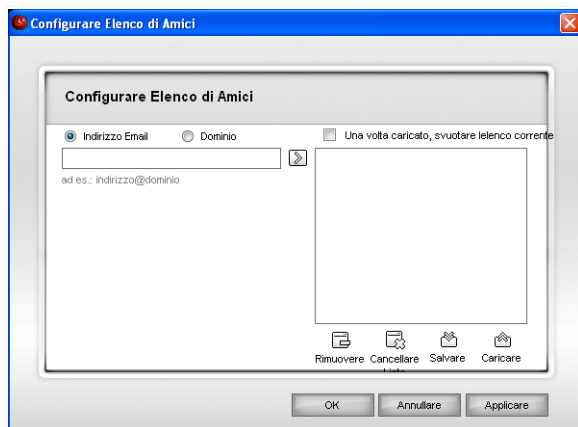
9.2.2. Passaggio 2/2 - Compilare l’ Elenco degli Indirizzi

Gli elenchi degli indirizzi contengono informazioni riguardanti gli indirizzi e-mail che vi inviano mail lecite o spam.

Elenco Amici

L'**Elenco Amici** è una lista di tutti gli indirizzi email dai quali volete sempre ricevere messaggi, indipendentemente dal loro contenuto. I messaggi provenienti dai vostri amici non verranno etichettati come spam, anche se il loro contenuto potrebbe assomigliare allo spam.

Nota
Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà auotomaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.

Per gestire l' **Elenco Amici** fare un click su (corrispondente all' **Elenco Amici**) o selezionare il bottone **Amici** dalla barra degli strumenti Antispam.

Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall’**Elenco Amici**.

Se desiderate aggiungere un indirizzo email, selezionate l' opzione **Indirizzo Email**, digitate l’indirizzo e premete il pulsante . L’indirizzo apparirà sull’**Elenco Amici**.

Importante

Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare dominio e premere il pulsante . Il dominio apparirà sull'**Elenco Amici**.

Importante

Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *domain* - tutte le mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *com - tutte le mail con il suffisso di dominio com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Amici** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; inoltre aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

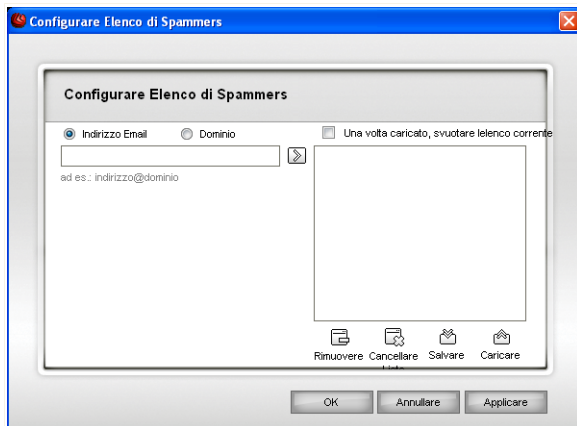
Selezionare **Applica** e **OK** per salvare e chiudere **l'Elenco Amici**.

Elenco Spammers

L'**Elenco Spammers** è l'elenco di tutti gli indirizzi e-mail dai quali non volete ricevere messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail ricevuta da un indirizzo contenuto nell'**Elenco Spammers** sarà automaticamente marcato come SPAM, senza alcun ulteriore processo.

Per gestire l'**Elenco Spammers** selezionare (in corrispondenza dell'**Elenco Spammers**) oppure premere il pulsante **Spammers** posizionato nella Barra degli strumenti Antispam.

Elenco Spammers

Qui potete aggiungere o rimuovere elementi dall'**Elenco Spammers**.

Se desiderate aggiungere un indirizzo email, selezionare il campo **Indirizzo Email**, inserire l'indirizzo e premere il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: name@domain.com.

Se volete aggiungere un dominio, selezionare l'opzione **Dominio**, digitare il nome e fare un click su . Il dominio apparirà nell'**Elenco Spammers**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com saranno marcate come SPAM;
- *domain* - tutte le mail provenienti da domain (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- *com - tutte le mail ricevute con il suffisso di dominio com verranno marcate come Spam.

Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

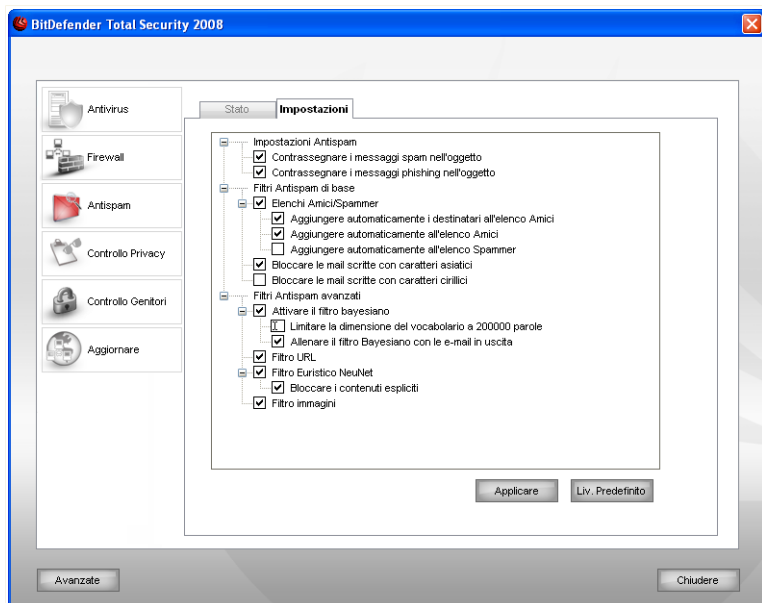
Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Spammers** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Selezionare **Appica** e **OK** per salvare e chiudere l' **Elenco Spammers**.

Importante
Se si desidera re-installare BitDefender, consigliamo di fare un salvataggio degli elenchi **Amici** / **Spammers** e quindi ricaricarli al termine del processo di re-installazione.

9.3. Impostazioni Antispam

Per configurare le impostazioni antispam, cliccare su **Antispam>Impostazioni** nel console di configurazione. Apparirà la finestra seguente:

Impostazioni Antispam

Qui potete abilitare/disabilitare ciascuno dei filtri Antispam e inoltre è possibile specificare alcune regolazioni relativa al modulo di Antispam.

Sono disponibili tre categorie di opzioni (**Impostazioni Antispam**, **Filtri Antispam** and **Filtri Avanzati Antispam**) organizzati come menu espandibili, simili a quelli di Windows.

Nota
Selezionare la casella con "+" per aprire una categoria oppure una casella con "-" per chiudere una categoria.

9.3.1. Impostazioni Antispam

- **Contrassegna i messaggi spam nell' oggetto** - tutti i messaggi email considerati come Spam saranno etichettati come SPAM nell' oggetto.
- **Marca l'oggetto dei messagi considerati phishing** - tutte le mail considerate messaggi di phishing saranno etichettate come SPAM sulla linea dell' oggetto.

9.3.2. Filtri Antispam

- **Elenchi Amici/Spammers** - attiva/disattiva gli Elenchi Amici/Spammers;
  - **Aggiungi automaticamente all'elenco degli Amici** - aggiunge automaticamente i mittenti all'Elenco Amici.
  - **Aggiungi Automaticamente all'Elenco Amici** - quando verrà premuto il pulsante **No Spam** dalla Barra degli strumenti Antispam il mittente verrà aggiunto automaticamente all' **Elenco Amici**.
  - **Aggiungi automaticamente all'elenco Spammer** - la prossima volta che si preme il pulsante **Spam** dalla Barra degli strumenti Antispam il mittente sarà automaticamente aggiunto all'**Elenco Spammers**.

Nota
I pulsanti **No spam** e **Spam** sono utilizzati per "istruire" il filtro Bayesiano.

- **Bloccare messaggi scritti in caratteri asiatici** - blocca i messaggi scritti in Caratteri Asiatici.
- **Bloccare messaggi scritti in caratteri cirillici** - blocca i messaggi scritti in Caratteri Cirillici.

9.3.3. Filtri Avanzati Antispam

- **Abilita il motore di Apprendimento (bayesiano)** - attiva/disattiva il Motore di Apprendimento (bayesiano).
  - **Limita la dimensione del dizionario a 200000 parole** - con questa opzione impostate la dimensione del dizionario Bayesiano – se minore è più veloce, se maggiore è più accurato.

Nota
La dimensione consigliata è: 200.000 parole.

  - **Istruisci il Motore di Apprendimento (bayesiano) per le e-mails in uscita** - istruisce il Motore di Apprendimento (bayesiano) per le e-mails in uscita.
- **Filtro URL** - attiva/disattiva il Filtro URL;
- **Filtro Euristico** - attiva/disattiva il Filtro Euristico;
  - **Blocco dei contenuti espliciti** - attiva/disattiva la scansione di messaggi "SESSUALMENTE ESPLICIT" nell'oggetto;
- **Filtro Immagini** - attiva/disattiva il Filtro Immagini.

Nota
Per attivare/disattivare una opzione, selezionare/pulire il checkbox corrispondente.

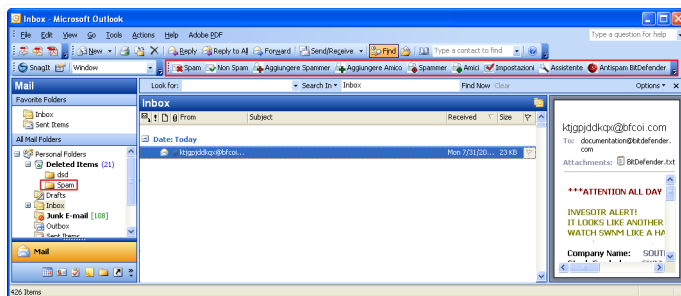
Selezionare **Applica** per salvare le modifiche oppure **Preimpostazione** per tornare alle impostazioni di default.

9.4. Integrazione nei client di posta

BitDefender si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti client di posta:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

9.4.1. Barra degli Strumenti Antispam

Nella parte superiore del vostro client di posta potete vedere la Barra degli Strumenti Antispam.

Barra degli Strumenti Antispam

Importante
La differenza tra BitDefender Antispam per Microsoft Outlook o Outlook Express/Windows mail consiste nel fatto che i messaggi SPAM sono spostati nella cartella **Spam** per Microsoft Outlook mentre per Outlook Express/Windows Mail sono spostati nella cartella **Elementi Cancellati**. In entrambi i casi i messaggi vengono etichettati come SPAM nella riga dell'oggetto.

La cartella **Spam** è creata automaticamente da BitDefender in Microsoft Outlook e viene inserita nel medesimo livello degli elementi dall' **Elenco Cartella**(Calendario, Contatti, ecc.)

Di seguito la spiegazione dei pulsanti nella barra degli strumenti BitDefender:

- **E' spam** - invia un messaggio al modulo Bayesiano indicando che la e-mail selezionata è spam. L'e-mail sarà marcata come SPAM e verrà spostata nella cartella **Spam**.

  I futuri messaggi e-mail con le stesse caratteristiche verranno marcati come SPAM.

  Nota
  E' possibile selezionare uno o più messaggi e-mail.

- **Non spam** - invia un messaggio al modulo Bayesiano indicando che la e-mail selezionata non è spam. BitDefender non dovrebbe classificarla. L'e-mail sarà spostata dalla cartella **Spam** alla directory **Inbox**.

  I futuri messaggi e-mail con le stesse caratteristiche non verranno marcati come SPAM.

  Nota
  E' possibile selezionare uno o più messaggi e-mail.

  Importante
  Il pulsante **Non spam** si attiva quando si seleziona un messaggio marcato come SPAM da BitDefender (normalmente questi messaggi sono situati nella cartella **Spam**).

- **Aggiungi spammer** - aggiunge il mittente della e-mail selezionata all' **Elenco Spammers**.

Aggiungi Spammer

Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando un indirizzo spammer viene aggiunto all'elenco.

Selezionare **OK** per chiudere la finestra.

Le future e-mail provenienti da quell' indirizzo saranno marcate come SPAM.

Nota
E' possibile selezionare uno o più mittenti.

- **Aggiungi Amici** - aggiunge il mittente della e-mail selezionata all' **Elenco Amici**.

Aggiungi Amici

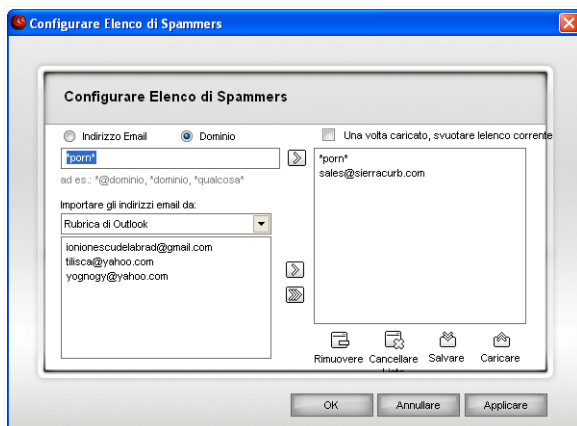
Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo all'elenco.

Selezionare **OK** per chiudere la finestra.

Riceverete sempre le email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Nota
E' possibile selezionare uno o più mittenti.

- **Spammers** - apre **l'Elenco Spammers** che contiene tutte gli indirizzi e-mail dai quali non si vogliono ricevere messaggi, indipendentemente dal loro contenuto.

Nota
Qualsiasi mail ricevuta da un indirizzo contenuto nell'**Elenco Spammers** sarà automaticamente marcato come SPAM, senza alcun ulteriore processo.

Elenco Spammers

Qui potete aggiungere o rimuovere elementi dall'**Elenco Spammers**.

Se si desidera aggiungere un indirizzo email, spuntare l' opzione **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante ⊡. L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante ⊡. Il dominio apparirà nell'**Elenco Spammers**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com saranno marcate come SPAM;
- *domain* - tutte le mail provenienti da domain (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- *com - tutte le mail ricevute con il suffisso di dominio com verranno marcate come Spam.

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina**Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express / Windows Mail** apparirà una nuova finestra dove potete selezionare la cartella che contiene gli indirizzi mail che volete aggiungere all'**Elenco Spammer**. Sceglieteli e cliccate su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare click su per aggiungerli all'**Elenco Spammers**. Facendo click su tutti gli indirizzi verranno aggiunti all' elenco.

Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

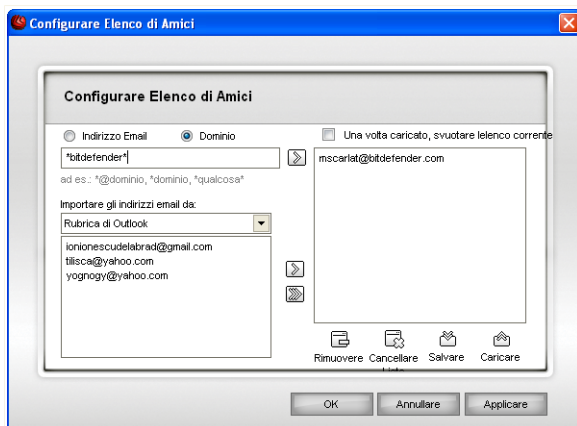
Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Spammers** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Selezionare **Appica** e **OK** per salvare e chiudere l' **Elenco Spammers**.

- **Amici** - apre l'**Elenco Amici** che contiene tutti gli indirizzi e-mail dai quali volete sempre ricevere i messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà auotomaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.

Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se si desidera aggiungere un indirizzo email, spuntare il campo **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Amici**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *domain* - tutte le mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *com - tutte le mail con il suffisso di dominio com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina**Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express** apparirà una nuova finestra dove potrete selezionare la cartella che contiene gli indirizzi mail che vorrete aggiungere all'**Elenco Amici**. Sceglierli e cliccare su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare click su per aggiungerli all'**Elenco Amici**. Facendo click su tutti gli idirizzi verranno aggiunti all'elenco.

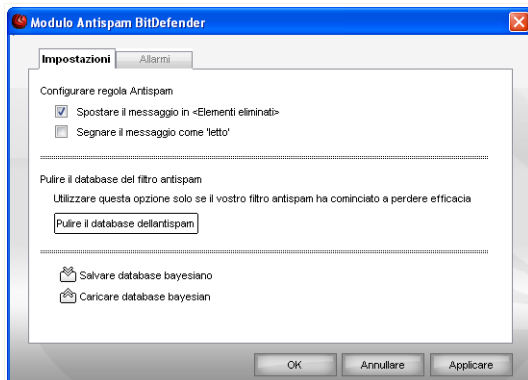
Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Amici** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Nota
Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; inoltre aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Selezionare **Applica** e **OK** per salvare e chiudere **l'Elenco Amici**.

- **Impostazioni** - apre la finestra **Impostazioni** dove potete specificare alcune opzioni per il modulo **Antispam**.

Impostazioni

Sono disponibili le seguenti opzioni:

- **Sposta il messaggio in Elementi Cancellati** - sposta i messaggi spam nella cartella **Elementi Cancellati** (solo per Microsoft Outlook Express / Windows Mail);
- **Marcare il messaggio come letto** - marca tutti i messaggi spam come letti così da non essere disturbati quando arrivano nuovi messaggi spam.

Se il vostro filtro antispam è molto impreciso, può rendersi necessario pulire il database del filtro e istruire nuovamente il Filtro Bayesiano. Selezionare **Pulisci il database dell'antispam** per resettare il Database Bayesiano.

Utilizzare i tasti **Salva Database Bayesiano**/ **Carica Database Bayesiano** per salvare/caricare l'elenco del Database Bayesiano nell'ubicazione desiderata. Il file avrà l'estensione `.dat`.

Selezionare la tabella **Avvisi** se si desidera accedere alla sezione dove è possibile disattivare la comparsa della finestra di conferma per i pulsanti **Aggiungi spammer** e **Aggiungi amici**.

Nota

Nella finestra **Avvisi** potete anche abilitare / disabilitare la comparsa dell'avviso **Seleziona un messaggio e-mail**. Questo avviso compare quando selezionate un gruppo invece di un messaggio e-mail.

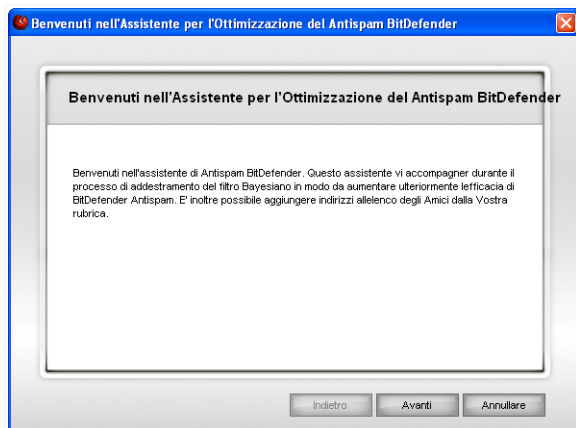
- **Interfaccia** - apre l' assistente che vi guidera attraverso il processo di istruzione del Filtro Bayesiano, così da incrementare l' efficienza dell' Antispam di BitDefender. Potete inoltre aggiungere indirizzi dalla vostra **Rubrica** all' **Elenco Amici** / **Elenco Spammers**.
- **BitDefender Antispam** - apre la Console di Gestione.

9.4.2. Assistente della Configurazione Antispam

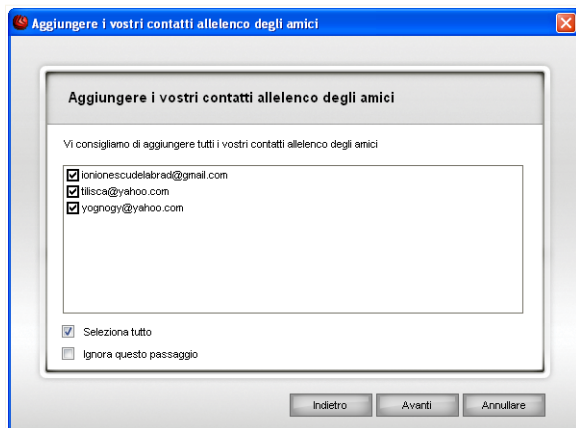
La prima volta che viene lanciato il vostro client di posta con BitDefender installato, apparirà l'assistente per aiutarvi a configurare l' Elenco Amici, l' Elenco Spammers e per istruire il Filtro Bayesiano in modo da aumentare l' efficienza dei filtri Antispam.

Nota

L'assistente può essere lanciato quando volete, cliccando sul tasto **Assistente** nella barra degli strumenti Antispam.

Passaggio 1/6 - Finestra di Benvenuto

Finestra di benvenuto

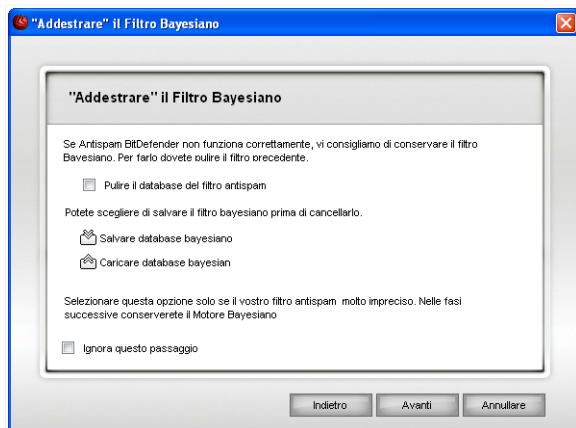
Selezionare **Avanti**.

Passaggio 2/6 - Compilare l' Elenco Amici

Compilare l' Elenco Amici

Da qui è possibile vedere tutti gli indirizzi della vostra **Rubrica**. Selezionare quelli che si intende aggiungere all' **Elenco Amici** (suggeriamo di selezionarli tutti). Riceverete tutti i messaggi e-mail provenienti da questi indirizzi, indipendentemente dal loro contenuto.

Per aggiungere tutti i vostri contatti all'elenco degli Amici, selezionare **Selezionare tutti**.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passaggio 3/6 - Cancellare il Database Bayesiano

Cancellare il Database Bayesiano

Potreste notare che il vostro Filtro Antispam ha iniziato a perdere efficienza. Questo potrebbe essere dovuto a una "istruzione" impropria. (per esempio nel caso in cui si sia erroneamente marcato un certo numero di messaggi legittimi come Spam o viceversa). Se il vostro filtro risulta molto inaccurato, potrebbe essere necessario pulire il database del filtro e istruirlo nuovamente, seguendo le fasi successive di questa procedura guidata.

Selezionare **Pulire il database del filtro antispam** se si desidera resettare il database Bayesiano.

Utilizzare i tasti **Salva database Bayesiano**/ **Carica database Bayesiano** per salvare / caricare il Database Bayesiano nell'ubicazione desiderata. Il file avrà l' estensione `.dat`.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passaggio 4/6 - Istruzione del Filtro Bayesiano con messaggi e-mail Leciti

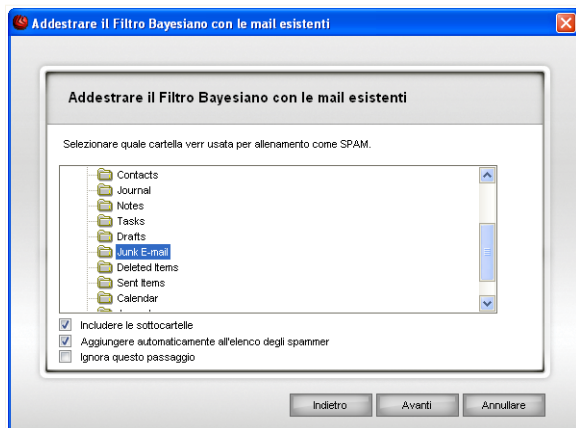
Istruzione del Filtro Bayesiano con messaggi e-mail Leciti

Selezionare una cartella che contenga messaggi e-mail leciti. Questi messaggi verranno utilizzati per istruire il filtro Antispam.

Ci sono due opzioni avanzate sotto la lista delle directory:

- **Includere sotto-cartelle** - per includere le sottocartelle alla vostra selezione.
- **Aggiungere automaticamente all'elenco degli amici** - per aggiungere i mittenti all'**Elenco Amici**.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passaggio 5/6 - Istruzione del Filtro Bayesiano con SPAM

Istruzione del Filtro Bayesiano con SPAM

Selezionare una cartella che contiene messaggi e-mail spam. Questi messaggi saranno utilizzati per istruire il filtro Antispam.

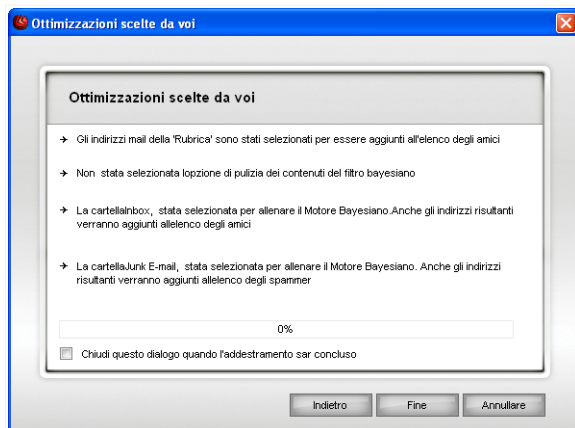
Importante

Assicurarsi che la cartella scelta contenga e-mail non lecite, altrimenti la prestazione antispam verrà ridotta considerevolmente.

Ci sono due opzioni avanzate sotto la lista delle directory:

- **Includere sotto-cartelle** - per includere le sottocartelle alla vostra selezione.
- **Aggiungi automaticamente all'elenco degli spammers** - per aggiungere i mittenti all'**Elenco Spammers**.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passo 6/6 – Sommario

Sommario

In questa finestra si possono vedere tutte le impostazioni dell'assistente di configurazione. Potrete eseguire qualsiasi modifica, tornando al passo precedente (selezionare **Indietro**).

Se non volete apportare alcuna modifica, selezionare **Fine** per terminare la procedura guidata di configurazione.

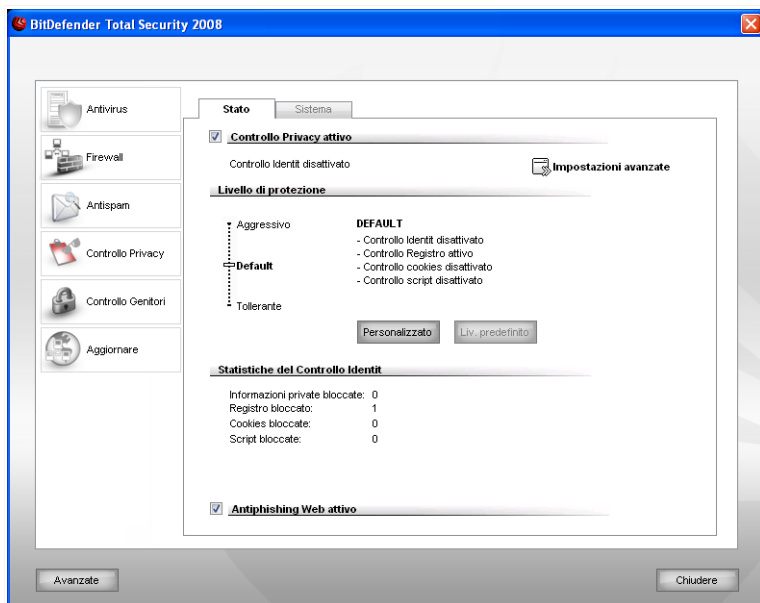
10. Controllo Privacy

BitDefender esegue il monitoraggio di dozzine di potenziali “hotspots” nel vostro sistema dove lo spyware potrebbe agire; inoltre analizza qualsiasi cambiamento avvenuto sia nel sistema che sul software. Le minacce dello spyware sono quindi bloccate in tempo reale. Il modulo è attivo e blocca Trojan o altri codici installati da hackers, nel tentativo di compromettere la vostra privacy inviando informazioni personali, quali numeri di carte di credito per esempio, dal vostro computer ad altri.

BitDefender esamina anche i siti web visitati ed avvisa se viene rilevata qualche minaccia di phishing.

La sezione **Controllo Privacy** di questa guida all’utente contiene i seguenti punti:

10.1. Stato Controllo Privacy

Per configurare il Controllo Privacy e visualizzare informazioni riguardanti la sua attività, cliccare su **Controllo Privacy>Stato** nel console di configurazione. Apparirà la finestra seguente:

Stato Controllo Privacy

10.1.1. Controllo Privacy

Importante
Per evitare che gli spyware infettino il vostro computer, mantenere il **Controllo Privacy** attivo.

Il Controllo Privacy protegge il vostro computer utilizzando 5 importanti controlli di protezione:

- Controllo Identità - protegge i vostri dati riservati filtrando tutto il traffico HTTP e SMTP in uscita secondo le regole da voi create nella sezione Identità.
- Controllo di Registro - chiede il vostro permesso ogni volta che un programma cerca di modificare una chiave di registro per essere eseguita all'avvio di Windows.
- Il Controllo dei Cookie quando è attivato, chiederà il vostro consenso ogni volta che un sito web tenterà di impostare un cookie.

- Il Controllo degli Script quando è attivato, chiederà il vostro consenso ogni volta che un sito web tenterà di attivare uno script o un altro contenuto attivo.

Per configurare le impostazioni per questi controlli, cliccare Impostazioni Avanzate.

Nel lato inferiore della sezione è possibile vedere le **Statistiche Controllo Privacy**.

Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Solo il **Controllo di Registro** è abilitato.
Default	**Controllo di Registro** e **Controllo identità** sono abilitati.
Aggressiva	**Controllo di Registro**, **Controllo Identità** e **Controllo degli Script** sono abilitati.

Potete personalizzare il livello di protezione cliccando su **Personalizza livello**. Nella finestra che apparirà, selezionate i controlli Antispyware che volete abilitare e cliccate su **OK**.

Cliccando su **Predefinito** verranno applicate le impostazioni di default.

10.1.2. Protezione Antiphishing

Phishing è un'attività criminale su Internet che utilizza tecniche sociali d'ingegneria per indurre la gente con l'inganno a fornire informazione personale.

Il più delle volte, i tentativi di phishing consistono nell'invio massiccio di e-mail che sostengono di arrivare da un'azienda affermata e legittima.Questi messaggi ingannevoli vengono inviati nella speranza che almeno qualcuno dei ricevitori, il cui profilo corrisponde con il target del phishing, venga persuaso a divulgare informazioni private.

Un messaggio di phishing presenta normalmente una questione relativa al vostro account on line. Cerca di convincervi a cliccare su un link, fornito nel messaggio, per accedere ad un sito web presumibilmente legittimo (in realtà contraffatto) dove vengono richieste informationi personali. Vi può venir chiesto, per esempio, di confermare

informazioni sull'account, come nome utente e password, e di fornire il numero del vostro conto bancario o il codice fiscale. A volte, per essere più convincente, il messaggio potrebbe fingere che il vostro account è stato o minaccia di essere sospeso se non usate il link fornito.

Il phishing fa anche uso di spyware, come i Troiani registratori di chiavi, per rubare informazioni sull'account direttamente dal vostro computer.

I principali obbiettivi del phishing sono i clienti dei servizi di pagamento on line, come eBay e PayPal, come anche le banche che offrono servizi on line. Recentemente, anche gli utenti di siti web di reti sociali sono stati presi di mira dal phishing per ottenere dati d'identificazione personale usati poi per il furto d'identità.

Per essere protetti dai tentativi antiphishing quando navigate su Internet, mantenere **Antiphishing** attivo. In questo modo, BitDefender esaminerà ogni sito web prima che accediate e vi avvertirà dell'esistenza di minacce di phishing. Può essere configurata una White List di siti web che non vogliate vengano esaminati da BitDefender.

Per gestire facilmente la protezione antiphishing e la White List , utilizzare la barra degli strumenti Antiphishing integrata nel Internet Explorer. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Barra degli Strumenti Antiphishing*» (p. 177).

10.2. Impostazioni Avanzate - Controllo Identità

Tenere sicuri i dati riservati è una questione importante che ci preoccupa tutti. I furto di dati ha tenuto il passo con lo siluppo delle comunicazioni via Internet e fa uso di nuovi metodi per ingannare le persone inducendole a dare via informazioni private.

Che sia la vostra e-mail o il numero della vostra carta di credito, quando finiscono nelle mani sbagliate tali informazioni possono recarvi danno: potete trovarvi affogati nei messaggi di spam o potreste essere sorpresi nell'accedere ad un conto svuotato.

Il**Controllo Identità** vi aiuta a tenere al sicuro i dati riservati. Esso scansiona il traffico HTTP o SMTP, o entrambi, alla ricerca di determinate stringhe che avete definito. Se viene trovata una corrispondenza, la pagina web o la mail corrispondente viene bloccata.

Viene fornito un supporto Multi-utente, in modo che nessun altro utente del sistema possa vedere le regole che avete configurato.

Le regole della privacy possono essere configurate nella sezione **Identità**. Per accedere a questa sezione, aprire la finestra **Impostazioni avanzate del Controllo Privacy** e quindi cliccare sulla sezione **Identità**.

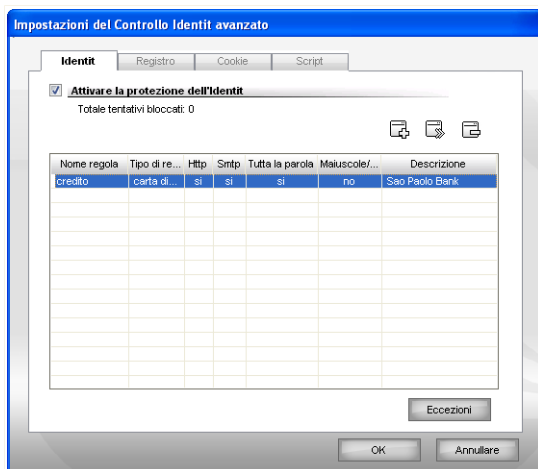
Nota

Per aprire la finestra **Impostazioni avanzate del Controllo Privacy**, cliccare su **Stato Controllo Privacy** nel console di configurazione e quindi cliccare su **Impostazioni Avanzate**.

Controllo Identità

10.2.1. Creazione delle Regole d'Identità

Le regole devono essere inserite manualmente(cliccando sul pulsante **Aggiungere** e scegliendo i parametri per le regole). Apparirà l'assistente di configurazione.

L'assistente di configurazione include una procedura di 3 passi.

Passaggio 1/3 - Impostazione Regola e Dati

Impostare il Tipo di Regola e i Dati

Inserire il nome della regola nel campo di editing.

Dovete impostare i parametri seguenti:

- **Tipo di Regola** - scegliere il tipo di regola (indirizzo, nome, carta di credito, PIN, SSN etc).
- **Dati della Regola** - inserire i dati della regola.

Nota
Se inserite meno di tre caratteri, vi verrà chiesto di validare i dati. Vi consigliamo di inserire al meno tre caratteri per evitare il blocco erroneo di messaggi e pagine web.

Tutti i dati che inserite sono criptati. Per una sicurezza maggiore, non inserire tutti i dati che volete proteggere.

Selezionare **Avanti**.

Passaggio 2/3 - Selezione del Traffico

Selezione del Traffico

Selezionare il traffico che si desidera esaminare con BitDefender. Sono disponibili le seguenti opzioni:

- **Indirizzi** - esamina il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
- **Scansione delle mail in uscita** - esamina il traffico SMTP (mail) e blocca le mail in uscita corrispondenti ai dati della regola.

Potete scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.

Selezionare **Avanti**.

Passo 3/3 – Definizione Regola

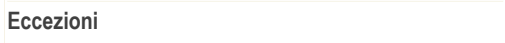
Definizione Regola

Inserire una breve descrizione della regola nel campo di editing.

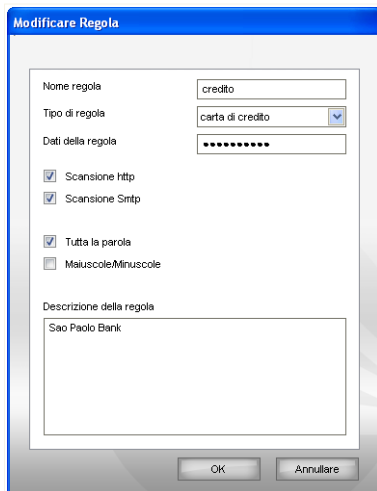
Selezionare **Termina**.

10.2.2. Definizione Eccezioni

Ci sono dei casi in cui dovrete definire eccezioni a specifiche regole d'identità. Consideriamo il caso in cui voi create una regola che impedisca l'invio attraverso HTTP (web) del numero della vostra carta di credito. Ogni volta che il numero della vostra carta di credito verrà inviato ad un sito web dal vostro account, la rispettiva pagina verrà bloccata. Se volete, per esempio, comprare delle scarpe in un negozio on line (che sapete che è sicuro), dovrete specificare un'eccezione alla rispettiva regola.

Per aprire la finestra dove si possono gestire l'eccezioni, cliccare su **Eccezioni**.

Eccezioni

Per aggiungere un'eccezione, seguire i seguenti passi:

1. Cliccare su **Aggiungere** per aggiungere una nuova entrata nella tabella.
2. Cliccare due volte su **Specificare indirizzi consentiti** e fornire gli indirizzi web o mail che si desidera aggiungere come eccezione.
3. Cliccare due volte su **Scegliere tipo** e scegliere dal menu l'opzione corrispondente al tipo d'indirizzo fornito in precedenza.
   - Se avete scelto un indirizzo web, selezionare **HTTP**.
   - Se avete scelto un indirizzo mail, selezionare **SMTP**.

Per rimuovere un'eccezione dall'elenco, selezionarla e quindi cliccare su**Rimuovere**.

Selezionare **Applica** per salvare le modifiche.

10.2.3. Amministrazione delle regole

Potete vedere l'elenco delle regole sulla scheda.

Per cancellare un elemento dall’elenco, selezionarlo e premere il pulsante **Rimuovi**. Per disattivare temporaneamente una regola senza cancellalrla, disattivare la casella corrispondente.

Per editare una regola, selezionarla e cliccare sul pulsante di Edit **Edit** oppure fare un doppio click. Apparirà una nuova finestra.

Modifica Regola

Qui potete modificare il nome, la definizione e i parametri della regola (tipo, dati e traffico). Cliccate su **OK** per salvare le modifiche.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

10.3. Impostazioni Avanzate - Controllo Registry

Una componente molto importante del sistema operativo di Windows si chiama **Registry**. Qui è dove Windows tiene le informazioni relative alle proprie configurazioni, ai programmi installati, all'utente e così via.

Il **Registry** è inoltre utilizzato per definire quali Programmi devono essere eseguiti automaticamente all'avvio di Windows. Spesso i virus lo utilizzano per essere eseguiti automaticamente quando l'utente riavvia il proprio computer.

Il **Controllo del Registry** sorveglia il Registry di Windows – azione utile per rilevare i Trojan (Cavalli di Troia). Vi avviserà ogni volta che un programma tenterà di modificare una entrata del registry per poter essere eseguito all'avvio di Windows.

Allarme sul Registry

E' possibile vietare questa modifica selezionando **No** oppure consentirla selezionando **Sì**.

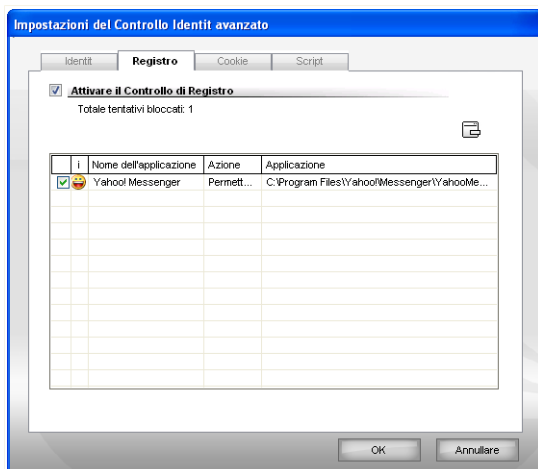
Se si desidera che BitDefender memorizzi questa risposta, selezionare **Applicare sempre questa azione a questo programma**. In questo modo, verrà creata una regola e la stessa azione verrà sempre appllicataogni volta che questo programma cerchi di modificare una chiave di registro per essere eseguita all'avvio di Windows.

Nota

BitDefender vi allerterà quando installerete nuovi programmi che necessitano di esecuzione immediata dopo il successivo avvio del vostro computer. Nella maggior parte dei casi questi programmi sono leciti e ci si può fidare.

Si potrà accedere ad ogni regola memorizzata nella sezione **Registro** per ulteriori migliorie. Per accedere a questa sezione aprire la finestra**Impostazioni Avanzate del Controllo Privacy** e quindi cliccare sulla sezione**Registro**.

Nota

Per aprire la finestra **Impostazioni avanzate del Controllo Privacy**, cliccare su **Stato Controllo Privacy** nel console di configurazione e quindi cliccare su **Impostazioni Avanzate**.

Controllo Registro

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e cliccare sul tasto **Rimuovi**. Per disattivare temporaneamente una regola senza eliminarla, deselezionare la casella corrispondente.

Per cambiare l'azione di una regola, cliccare due volte sul campo dell'azione e selezionare l'opzione appropriata dal menu.

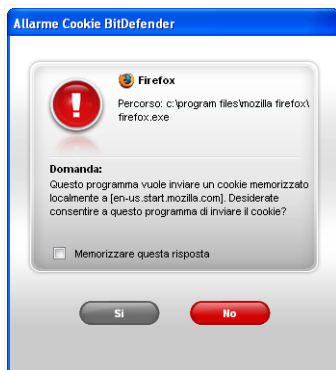
Selezionare **OK** per chiudere la finestra.

10.4. Impostazioni Avanzate - Controllo Cookie

I Cookies sono molti frequenti su Internet. Si tratta di piccoli files immagazzinati sul vostro computer. I siti web creano questi cookies per mantenere traccia di specifiche informazioni che vi riguardano.

Generalmente i Cookies vengono creati per rendere facilitare la navigazione nei siti web. Ad esempio possono aiutare i siti web a ricordare il vostro nome e le vostre preferenze, evitandovi così di doverli inserire ad ogni visita.

I cookie però possono anche essere utilizzati per compromettere la vostra privacy, tenendo traccia delle vostre abitudini di navigazione.

E' in questo caso che il **Controllo dei Cookies** vi sarà di aiuto. Quando è attivato, il **Controllo dei Cookies** chiederà il vostro consenso ogni volta che un sito web tenta di impostare un cookie:

Allarme Cookie

E' possibile visualizzare il nome dell'applicazione che sta tentando di inviare un file cookie.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando ci si collegherà successivamente allo stesso sito.

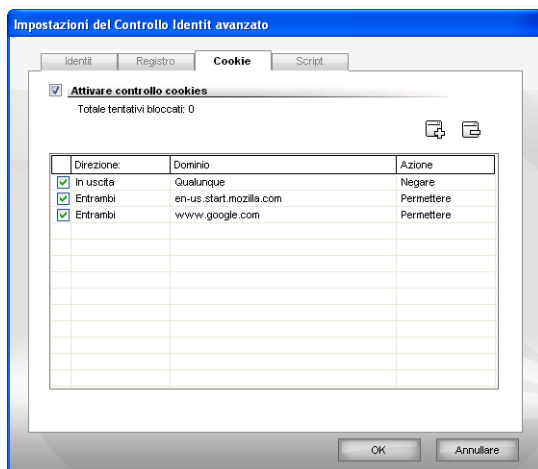
Questo vi aiuterà a scegliere i siti web di cui fidarsi o no.

Nota

A causa del notevole numero di cookie utilizzati oggi giorno su Internet, il **Controllo dei Cookies** può risultare inizialmente abbastanza noioso. All'inizio porrà molte domande riguardo ai siti che tentano di piazzare i cookies sul vostro computer. Non appena si aggiungeranno i vostri siti abituali all'elenco delle regole, la navigazione diventerà semplice come prima.

E' possibile accedere a qualsiasi regola memorizzata nella sezione **Cookies** per ulteriori perfezionamenti. Per accedere a questa sezione, aprire la finestra **Impostazioni Avanzate del Controllo dellla Privacy** e cliccare la sezione **Cookie**.

Nota

Per aprire la finestra **Impostazioni avanzate del Controllo Privacy**, cliccare su **Stato Controllo Privacy** nel console di configurazione e quindi cliccare su **Impostazioni Avanzate**.

Controllo Cookie

Potete visualizzare l'elenco delle regole create finora nella tabella.

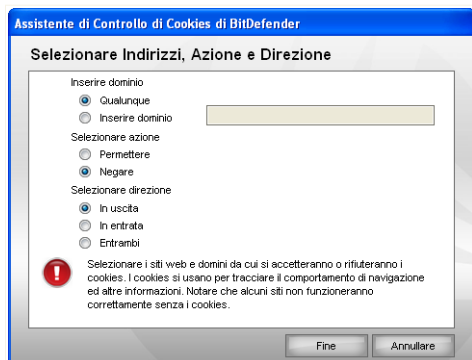
Importante
La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare i parametri di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondente.

Le regole possono essere immesse automaticamente (attraverso la finestra di avviso) o manualmente (cliccare sul pulsante **Aggiungi** e scegliere i parametri per la regola). Apparirà l'assistente di configurazione.

10.4.1. Assistente per la Configurazione

Assistente per la Configurazione consiste in una procedura di un solo passo.

Passo 1/1 - Selezione Indirizzo, Azione e Direzione

Selezione Indirizzo, Azione e Direzione

Potete impostare i parametri:

- **Indirizzo Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	*Descrizione*
Abilitazione	I cookies da quel dominio verranno eseguiti.
Impedisci	I cookies da quel dominio non verranno eseguiti.

- **Direzione** - seleziona la direzione del traffico.

Tipo	*Descrizione*
In Uscita	La regola sarà applicata solo ai cookies che vengono rispediti al sito connesso.
In Entrata	La regola sarà applicata solo ai cookies che vengono ricevuti dal sito connesso.
Entrambe	La regola sarà applicata in entrambe le direzioni.

Selezionare **Termina**.

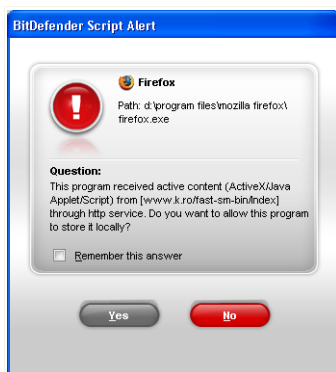
Nota
Si possono accettare i cookie, ma non conviene mai rispedirli, impostando l'azione **Divieto** e la direzione **In uscita**.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

10.5. Impostazioni Avanzate - Controllo Script

Gli Scripts e altri codici come ActiveX controls e Java applets, che sono utilizzati per creare pagine interattive, possono essere programamti per avere effetti dannosi. Per esempio gli elementi ActiveX , possono ottenere l' accesso ai dati del vostro computer, cancellare informazioni, catturare passwords e intercettare messaggi mentre siete online. Dovreste accettare contenuti attivi esclusivamente da siti che si conoscono come affidabili.

BitDefender vi consente di scegliere se eseguire questi elementi oppure bloccare la loro esecuzione.

Con il **Controllo degli Script** sarete voi a decidere quali siti web sono affidabili e quali no. BitDefender chiederà il vostro consenso ogni volta che un sito web tenterà di attivare uno script o altri contenuti attivi:

Allarme Script

E' possibile visualizzare il nome della risorsa.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando lo stesso sito tenterà di inviarvi contenuti attivi.

E' possibile accedere a qualsiasi regola memorizzata dalla sezione **Script** per ulteriori perfezionamenti. Per accedere a questa sezione, aprire la finestra **Impostazioni Avanzate del Controllo Privacy** e cliccare la sezione **Script**.

Nota
Per aprire la finestra **Impostazioni avanzate del Controllo Privacy**, cliccare su **Stato Controllo Privacy** nel console di configurazione e quindi cliccare su **Impostazioni Avanzate**.

Controllo degli Script

Potete visualizzare l'elenco delle regole create finora nella tabella.

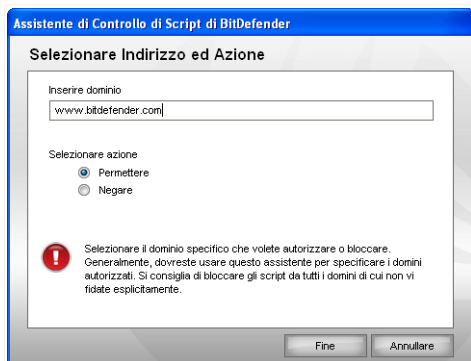
Importante
La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare i parametri di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondente.

Le regole possono essere immesse automaticamente (attraverso la finestra di avviso) o manualmente (cliccare sul pulsante **Aggiungi** e scegliere i parametri per la regola). Apparirà l'assistente di configurazione.

10.5.1. Assistente per la Configurazione

Assistente per la Configurazione consiste in una procedura di un solo passo.

Passaggio 1/1 - Selezione Indirizzo ed Azione

Selezione Indirizzo e Azione

Potete impostare i parametri:

- **Indirizzo Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Abilitazione	Gli scripts da quel dominio saranno eseguiti.
Impedisci	Gli scripts da quel dominio non saranno eseguiti.

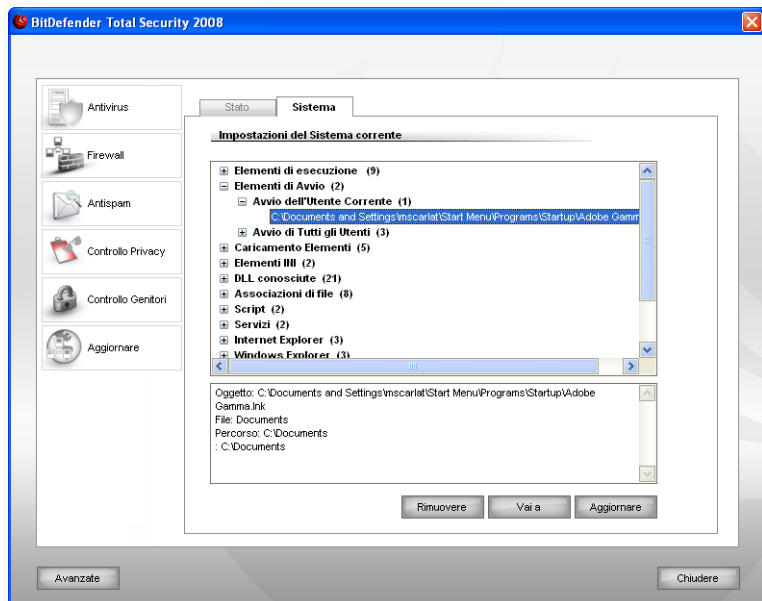
Selezionare **Termina**.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

10.6. Sistema di Informazione

BitDefender vi permette di visualizzare, da una singola ubicazione, tutta la configurazione del sistema e le applicazioni che verranno eseguite all'avvio. In questo

modo potrete monitorare l'attività del sistema e delle applicazioni installate così come identificare possibili infezioni del sistema.

Per ottenere informazioni sul sistema cliccare su **Controllo Privacy>Informazioni di Sistema** nel console di configurazione. Apparirà la finestra seguente:

Sistema di Informazione

La lista contiene sia gli elementi caricati all' avvio del sistema che quelli caricati da applicazioni diverse.

Sono disponibili tre pulsanti:

- **Rimuovi** - cancella l'elemento selezionato. Cliccare **Sì** per confermare la vostra scelta.

Nota
Se desiderate che non vi venga chiesto di nuovo di confermare la vostra scelta durante la sessione corrente, selezionare **Non chiedermi di nuovo in questa sessione**.

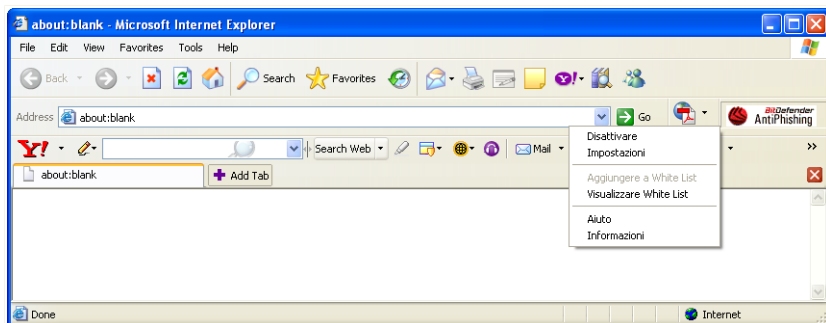
- **Vai a** - apre una finestra dove e situato l'elemento selezionato (la **Registy** ad esempio).
- **Aggiorna** - riapre la sezione del **Sistema Informazione**.

10.7. Barra degli Strumenti Antiphishing

BitDefender vi protegge da tentativi di phishing mentre navigate in Internet. Esamina i siti web visitati e vi allerta se ci sono minacce di phishing. Può essere configurata una White List di siti web che non vogliate vengano esaminati da BitDefender.

Potete gestire facilmente ed efficacemente la protezione antiphishing e la White List utilizzando la barra degli strumenti Antiphishing BitDefender integrata nell'Internet Explorer.

La barra degli strumenti antiphishing, rappresentata dall' **icona BitDefender**, si trova nella parte superiore dell'Internet Explorer. Cliccare sopra per aprire il menu della barra degli strumenti.

Nota
Se non potete visualizzare la barra degli strumenti, aprire il menu **Visualizzare**, puntare su **Barre degli strumenti** e selezionare **Barra degli strumenti BitDefender**.

Barra degli Strumenti Antiphishing

Nella barra degli strumenti sono disponibili i seguenti comandi:

- **Attivare / Disattivare** - attiva / disattiva la barra degli strumenti Antiphishing BitDefender.

Nota
Se scegliete di disattivare la barra degli strumenti Antiphishing, non sarete più protetti dai tentativi di phishing.

- **Impostazioni** - apre una finestra dove potete specificare le impostazioni della barra degli strumenti Antiphishing.

  Sono disponibili le seguenti opzioni:
  - **Attivare Scancione** - attiva la scansione antiphishing.
  - **Chiedere prima di aggiungere alla White List** - vi viene chiesto prima di aggiungere un sito web alla White List.
- **Aggiungere alla White List** - aggiunge il sito web corrente alla White List.

Nota
Aggiungere un sito alla White List significa che BitDefender non esaminerà più il sito per tentativi di phishing. Vi consigliamo di aggiungere alla White List solo siti di cui vi fidate pienamente.

- **Visualizzare White List** - apre la White List.

  Potete vedere la lista di tutti i siti web che non vengono controllati dai motori di antiphishing BitDefender.

  Se volete rimuovere un sito dalla White List in modo che vi sia notificata qualsiasi minaccia di phishing su quella pagina, cliccare sul tasto **Rimuovere**.

  Potete aggiungere i siti di cui vi fidate pienamente alla White List, in modo che non verranno più esaminati dai motori antiphishing. Per aggiungere un sito alla White List, inserire il suo indirizzo nel campo corrispondente e quindi cliccare **Aggiungere**.
- **Aiuto** - apre il file di aiuto.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.

11. Controllo Genitori

Il modulo Controllo Genitori può bloccare l'accesso a pagine siti web, e-mails che ritenete inappropriate, oppure l'accesso ad Internet (per alcuni periodi di tempo, come durante le ore dedicate ai "compiti di scuola") e impedire l'uso di applicazioni come giochi, chat, programmi con condivisione di file e altro.

Importante

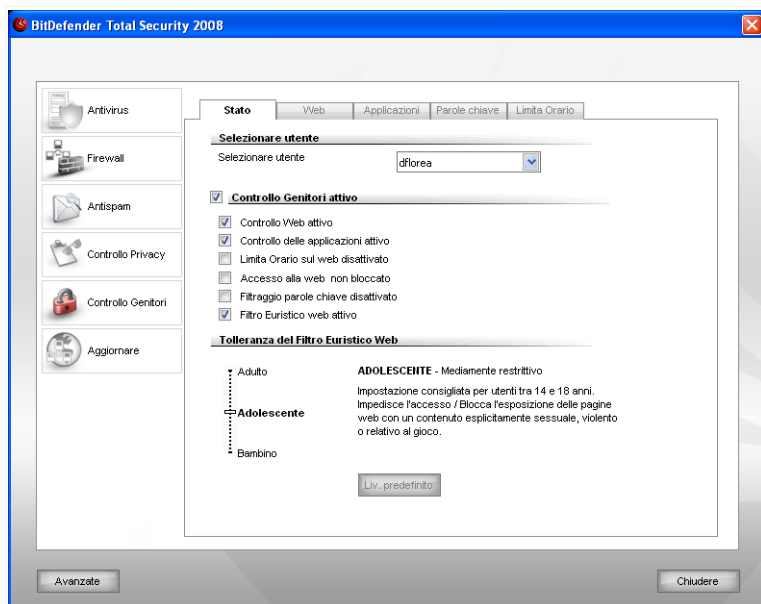
È possibile accedere e configurare questo modulo solo da parte di utenti con diritti di amministratore (amministratori di sistema). Se le impostazioni sono protette da password, esse possono essere modificate solo se la password è fornita. Un amministratore non può imporre un set di regole ad un utente per il quale siano state definite regole in precedenza da un altro amministratore.

Se non siete l'unica persona ad utilizzare questo computer, consigliamo di proteggere le vostre Impostazioni BitDefender con una password. Per impostare una password, cliccare Avanzate nel console di configurazione ed utilizzare l'opzione **Attivare protezione password per le impostazioni del prodotto**.

La sezione **Controllo Genitori** di questa guida all'utente contiene i seguenti punti:

- Stato Controllo Genitori
- Controllo Web
- Controllo Applicazioni
- Filtro parola chiave
- Limitatore Tempo sul Web

11.1. Stato del Controllo Genitori

Per configurare il Controllo Genitori per un utente selezionato, cliccare su **Controllo Genitori>Stato** nel console di configurazione. Apparirà la finestra seguente:

Stato del Controllo Genitori

Importante
Mantenere il **Controllo Genitori** abilitato per proteggere i vostri bambini dai contenuti inopportuni utilizzando le vostre regole di accesso al computer personalizzate.

11.1.1. Selezione dei Controlli di Protezione

Per configurare il livello di protezione dovete prima selezionare l'utente a cui volete applicare queste impostazioni. Quindi configurate il livello di protezione utilizzando i seguenti controlli:

- **Controllo Web** - abilitate il **Controllo Web** per filtrare la navigazione sul web secondo le regole da voi impostate nella sezione Web.
- **Controllo Applicazioni** - abilitate il **Controllo Applicazioni** per bloccare l'accesso alle applicazioni sul vostro computer secondo le regole da voi impostate nella sezione Applicazioni.
- **Limita Orario su Web** - abilitate il **Limita Orario su Web** per consentire l'accesso al web secondo l'orario da voi stabilito nella sezione Limitatore Tempo.

- **Accesso Web** - abilitate questa opzione per bloccare l'accesso a tutti i siti web (non solo a quelli nella sezione Web).
- **Filtraggo Parola Chiave** - abilitate il **Filtraggio Parola Chiave** per filtrare l'accesso al web e alla posta secondo le regole da voi impostate nella sezione Parole Chiave.
- **Filtro web euristico** - abilitate questa opzione per filtrare l'accesso al web secondo le regole prestabilite sulla base delle categorie di età.

Nota
Per usufruire completamente delle caratteristiche offerte dal Controllo Genitori, dovete configurare i controlli selezionati.

11.1.2. Configurazione del Filtro Euristico Web.

Il Filtro Euristico Web analizza le pagine web e blocca quelle che corrispondono a modelli dal contenuto potenzialmente inappropriato.

Potete impostare il livello di protezione usando i set di regole predefiniti in base all'età per filtrare l'accesso web oppure selezionare certe categorie di contenuti alle quali bloccare l'accesso.

Trascinate il pulsante scorrevole lungo la barra per impostare il livello di protezione che considerate appropriato per l'utente selezionato.

Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Bambino	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti al di sotto dei 14 anni. Le pagine web con contenuto potenzialmente dannoso per i bambini (porno, sessualità, droghe, hacking ecc.) sono bloccate.
Adolescenti	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti con età tra i 14 e i 18 anni. Le pagine web con contenuto sessuale, pornografico o per adulti sono bloccate.
Adulti	Offre un accesso illimitato a tutte le pagine web indipendentemente dal loro contenuto.

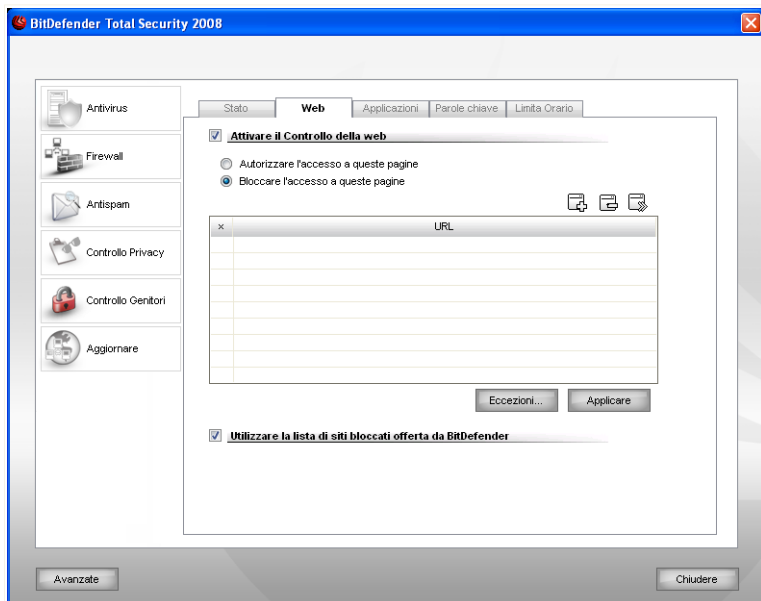
Cliccare su **Personalizza Livello** per impostare le vostre regole di filtraggio personalizzate. Nella finestra che apparirà, selezionate le categorie di contenuto (gioco

d'azzardo, hacking, porno ecc) per le quali BitDefender deve impedire l'accesso su web da parte dell'utente e cliccare su **OK**.

Cliccare su **Livello di Default** per impostare il pulsante scorrevole al livello di default.

11.2. Controllo Web

Il **Web Control** ti aiuta a bloccare l'accesso ai siti web inappropriati. Una lista di utenti per bloccare i siti inappropriati e una parte é fornita e aggiornata da BitDefender come parte del processo di aggiornamento regolare.

Per configurare il Controllo Web, cliccare **Controllo Genitori>Web** nel console di configurazione. Apparirà la finestra seguente:

Controllo Web

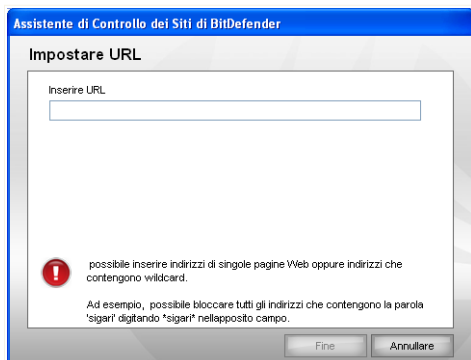
Per abilitare questa protezione selezionate la casella di controllo che corrisponde a **Abilita il Controllo Web**.

Selezionate **Consenti l'accesso a queste pagine**/**Blocca l'accesso a queste pagine** per vedere l'elenco dei siti permessi/bloccati. Cliccate su **Eccezioni** per accedere ad una finestra in cui potete vedere l'elenco complementare.

Le regole devono essere inserite manualmente. Prima di tutto, selezionate **Consenti accesso a queste pagine**/**Blocca accesso a queste pagine** per consentire/bloccare l'accesso ai siti web che specificherete nell'assistente. Quindi, cliccate sul pulsante **Aggiungi...** per avviare l'assistente di configurazione.

11.2.1. Assistente per la Configurazione

Assistente per la Configurazione consiste in una procedura di un solo passo.

Passo 1/1 – Specificare i siti web

Specifica i siti web

Digitare il sito web per il quale la regola sarà applicata e cliccare su **Fine**.

Importante

Sintassi:

- `*.xxx.com` - l'azione della regola si applicherà a tutti i siti web che terminano con `.xxx.com`;
- `*porn*` - l'azione della regola sarà applicata in tutti i siti web che contengono `porn` nell'indirizzo del sito web;
- `www.*.com` - l'azione della regola sarà applicata in tutti i siti web aventi come suffisso del dominio `com`;

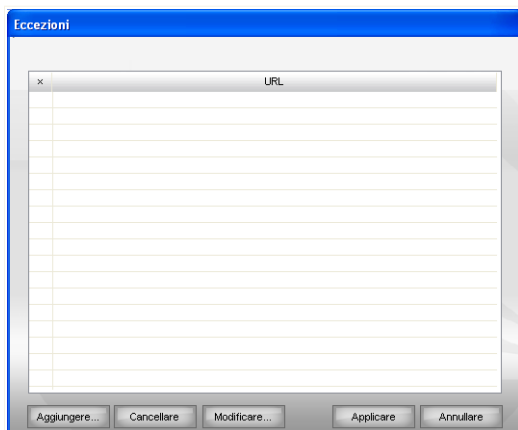
- `www.xxx.*` - l'azione della regola sarà applicata in tutti i siti web che iniziano con `www.xxx.` indipendentemente dal suffisso del dominio.

Cliccare **Applica** per salvare le modifiche.

Per cancellare una regola, selezionarla semplicemente e cliccare sul pulsante **Cancella**. Per modificare una regola selezionarla e cliccare sul pulsante **Modifica...** o fare doppio clic su di esso. Per disattivare temporaneamente una regola senza cancellarla, pulire la casella di spunta corrispondente.

11.2.2. Specifica Eccezioni

A volte potreste aver bisogno di specificare delle eccezioni ad una regola particolare. Ad esempio, avete impostato una regola che blocca i siti che contengono la parola "killer" nell'indirizzo (sintassi: `*killer*`). Siete anche coscienti dell'esistenza di un sito chiamato `killer-music` dove i visitatori possono ascoltare musica on-line. Per fare un eccezione alla regola precedentemente creata, accedete alla finestra **Eccezioni** e definite un'eccezione alla regola.

Cliccare su **Eccezioni...**. Apparirà la seguente finestra:

Specificare Eccezioni

Cliccare su **Aggiungi...** per specificare le eccezioni. L' assistente di configurazionek apparirà. Completare la procedura guidata per impostare l'eccezione.

Cliccare **Applica** per salvare le modifiche.

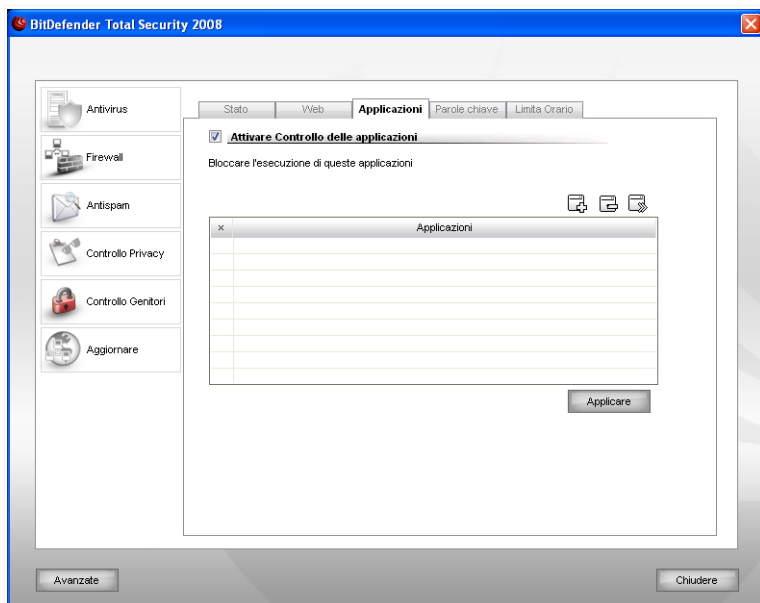
Per cancellare una regola, basta solo selezionarla e fare click su **Cancella**. Per modificare una regola, selezionarla e cliccare su **Modifica...** o fare doppio click. Per disattivare temporaneamente una regola senza eliminarla, pulite la casella di spunta corrispondente.

11.2.3. Blacklist Web BitDefender

Per aiutarvi a proteggere i vostri bambini, BitDefender fornisce una blacklist di siti web con contenuto inopportuno o probabilmente dannoso. Per bloccare i siti che appaiono in questo elenco selezionate **Utilizza l'elenco di siti bloccati fornito da BitDefender**.

11.3. Controllo Applicazioni

Il **Controllo Applicazioni** ti aiuta a bloccare qualsiasi applicazione in esecuzione. Giochi, messaggi software, oltre ad altre categorie di software e minacce che in questo caso possono essere bloccati. Le applicazioni bloccate sono così protette da modifiche, e non possono essere copiate o spostate.

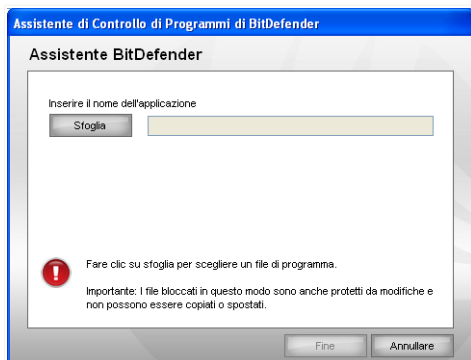
Per configurare il Controllo Applicazioni, cliccare **Controllo Genitori>Applicazioni** nel console di configurazione. Apparirà la finestra seguente:

Controllo Applicazioni

Per abilitare questa protezione seleziona la casella di controllo che corrisponde a **Abilita Controllo Applicazioni**.

Le regole devono essere inserite manualmente. Cliccare sul pulsante **Aggiungi...** per avviare la procedura di configurazione guidata.

11.3.1. Assistente per la Configurazione

Assistente per la Configurazione consiste in una procedura di un solo passo.

Passo 1/1 – Seleziona l'Applicazione da Bloccare

Seleziona l'Applicazione da Bloccare

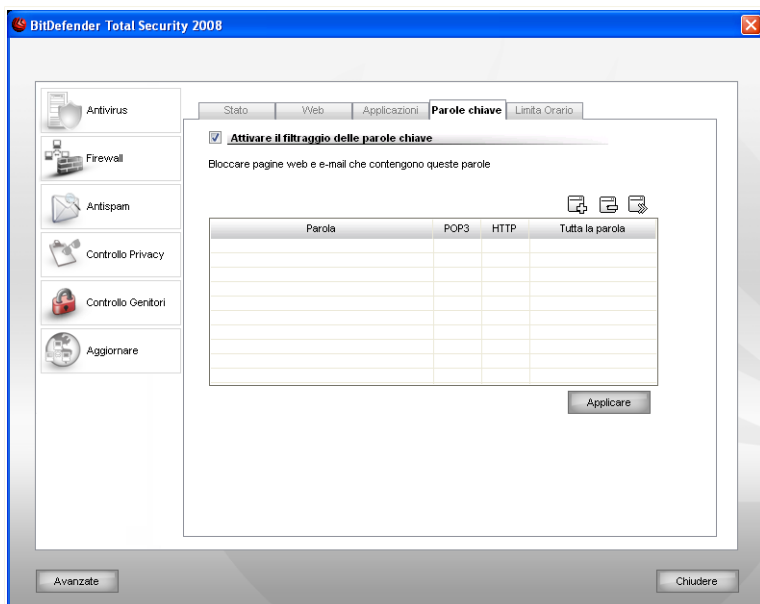
Cliccate su **Esplora**, selezionate l'applicazione da bloccare e cliccate su **Fine**.

Cliccare **Applica** per salvare le modifiche.

Per cancellare una regola, selezionarla semplicemente e cliccare sul pulsante **Cancella**. Per modificare una regola selezionarla e cliccare sul pulsante **Modifica...** o fare doppio clic su di esso. Per disattivare temporaneamente una regola senza cancellarla, pulire la casella di spunta corrispondente.

11.4. Filtraggio Parola Chiave

Il **Filtro Parola Chiave** vi aiuta a bloccare l'accesso ai messaggi e-mail o alle pagine web che contengono una parola specifica. In questo modo potete evitare che gli utenti vedano parole o frasi inopportune.

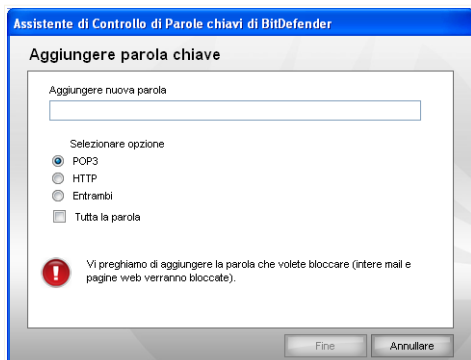
Per configurare il Filtraggio Parola Chiave, cliccare su **Controllo Genitori>Parole Chiavi** nel console di configurazione. Apparirà la finestra seguente:

Filtraggio Parola Chiave

Per abilitare questa protezione selezionate la casella di spunta che corrisponde a **Filtraggio Parola Chiave**.

Le regole devono essere inserite manualmente. Cliccare sul pulsante **Aggiungi...** per avviare la procedura di configurazione guidata.

11.4.1. Assistente per la Configurazione

L'assistente di configurazione comprende una procedura di 3 passi.

Passo 1/1 - Inserire la Parola Chiave

Inserite la parola chiave

Dovete impostare i parametri seguenti:

- **Parola chiave** - digitare nel campo di edit la parola o la frase che volete bloccare.
- **Protocollo** - scegliere il protocollo che BitDefender dovrebbe scansionare per la parola sepcificata.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
POP3	I messaggi e-mail che contengono la parola chiave sono bloccati.
HTTP	Le pagine web che contengono la parola chiave sono bloccate.
Entrambe	sia i messaggi e-mail che le pagine web che contengono la parola chiave sono bloccate.

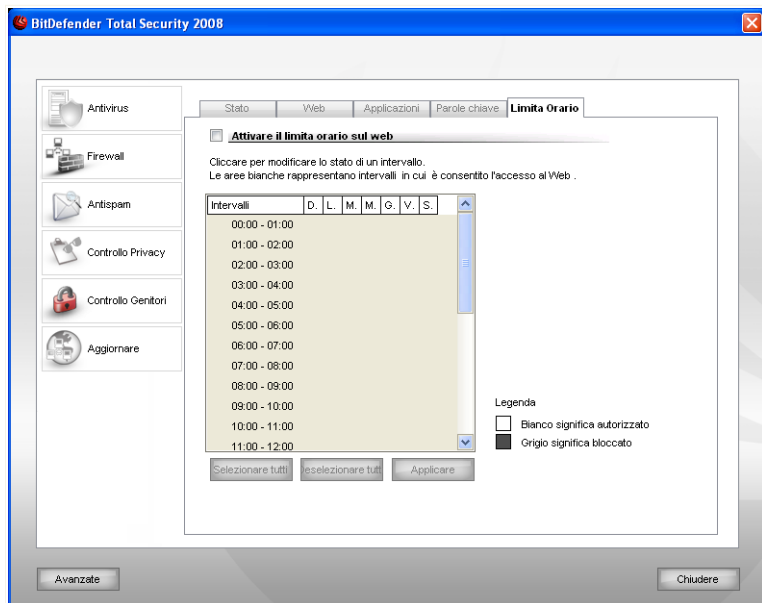
Cliccare **Applica** per salvare le modifiche.

Per cancellare una regola, selezionarla semplicemente e cliccare sul pulsante **Cancella**. Per modificare una regola selezionarla e cliccare sul pulsante **Modifica...** o fare doppio clic su di esso. Per disattivare temporaneamente una regola senza cancellarla, pulire la casella di spunta corrispondente.

11.5. Tempo limitato sul web

Il **Tempo limitato sul web** ti aiuta a bloccare l’accesso a internet per determinati periodi di tempo.

Nota
BitDefender eseguirà aggiornamenti ogni ora indipendentemente dall'impostazione **Tempo limitato sul web**.

Per configurare il Limita Orario sul web, cliccare su **Controllo Genitori>Limita Orario** nel console di configurazione. Apparirà la finestra seguente:

Tempo limitato sul web

Per abilitare questa protezione seleziona la casella di controllo che corrisponde a **Abilita Tempo limitato sul web**.

Seleziona l’intervallo di tempo quando sei connesso a internet, sarà così bloccato. Tu puoi cliccare su celle individuali, o puoi bloccare l’intervallo per un lungo periodo di

tempo. È possibile fare clic su **Controla tutto** per selezionare tutte le caselle e, implicitamente, bloccare tutto l'accesso alla rete. Se si fa clic su **Non controllare tutto**, le connessioni a Internet verranno consentite sempre.

Importante
I box colorati in grigio rappresentano l'intervallo di tempo quando la connessione internet è bloccata.

Cliccare **Applica** per salvare le modifiche.

12. Aggiornamento

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

Se siete connessi ad Internet con banda larga o DSL, BitDefender si prenderà cura di sè da solo. Per default, esso cercherà degli aggiornamenti, ogni volta che avvierete il vostro computer ed ogni **ora**dopo l'avvio.

Se è stato rilevato un aggiornamento, secondo le opzioni impostate nella sezione di Aggiornamento Automatico, vi verrà chiesto di confermare l' aggiornamento oppure verrà eseguito automaticamente.

Il processo di aggiornamento viene eseguito involo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodottoe, nello stesso tempo, ogni vulnerabilità verrà esclusa.

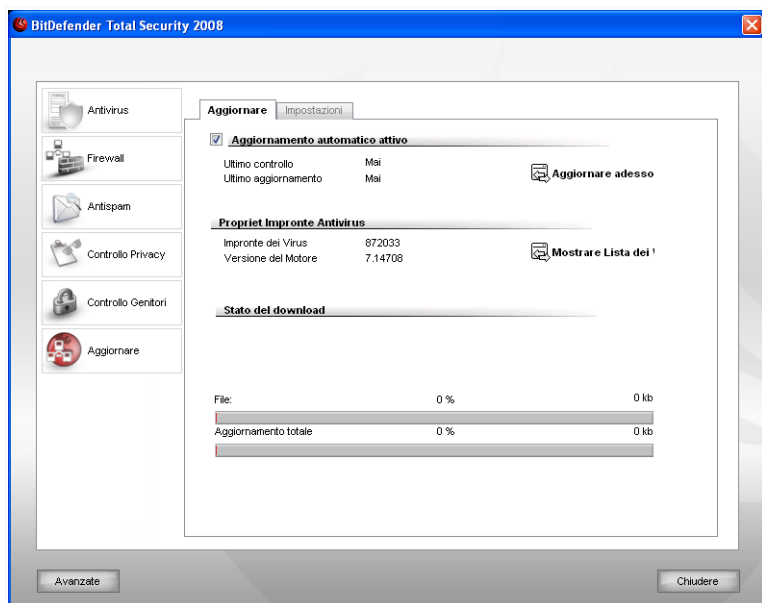
Gli aggiornamenti avvengono nei seguenti modi:

- **Aggiornamenti per motori Antivirus** - non appena compaiono nuove minacce, i files contenenti l'impronta dei virus devono essere aggiornati per garantire una protezione permanente in tempo reale. Questo tipo di aggiornamento è anche conosciuto come **Virus Definitions Update**.
- **Aggiornamenti per motori Antispam** - verranno aggiunte nuove regole ai filtri Euristico ed URL, e nuove immagini al filtro Immagini. Ciò contribuirà ad aumentare l'efficacia del vostro motore Antispam. Questo tipo di aggiornamento è anche conosciuto come **Antispam Update**.
- **Aggiornamento per i motori antispyware** - nuove impronte antispyware saranno aggiunte al database. Questo tipo di aggiornamento è anche conosciuto come **Aggiornamento Antispyware**.
- **Aggiornamenti del prodotto** - quando viene rilasciata la nuova versione di un prodotto, vengono introdotte nuove funzionalità e tecniche di scansione al fine di migliorarne l'efficienza. Questo tipo di aggiornamento è anche conosciuto come **Product Update**.

La sezione **Update** di questa guida all'utente comprende i seguenti argomenti:

- Aggiornamento Automatico
- Impostazioni dell'Aggiornamento

12.1. Aggiornamento Automatico

Per visualizzare informazioni relative all'aggiornamento ed eseguire aggiornamenti automatici, cliccare su **Aggiornamento>Aggiornamento** nel console di configurazione. Apparirà la finestra seguente:

Aggiornamento Automatico

Qui è possibile visualizzare quando sono stati eseguiti l'ultimo controllo degli aggiornamenti e l'ultimo aggiornamento, così come le informazioni sull'ultimo aggiornamento eseguito (se con successo o gli errori verificatisi). Inoltre si mostrano informazioni sulla versione del motore corrente ed il numero di impronte.

Potete verificare le impronte dei malware del vostro BitDefender cliccando **Mostrare Elenco dei Virus**.Verrà creato e aperto in un browser web un file HTML che contiene tutte le impronte disponibili. Potete cercare le impronte di uno specifico malware attraverso il database oppure clicare **Lista dei Virus BitDefender** per andare al database on line delle impronte di BitDefender.

se aprite questa sezione durante un aggiornamento potrete visualizzare lo stato del download.

Importante
Per essere sempre protetti, tenete l' **Aggiornamento Automatico** abilitato.

12.1.1. Richiedere un aggiornamento

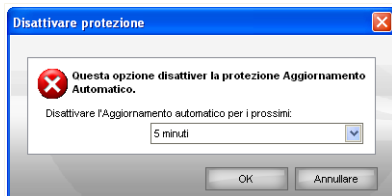
L'aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiorna adesso**. Questo aggiornamento è conosciuto anche come **Aggiornamento su richiesta dell'utente**.

Il modulo **Aggiornamento** si collegherà al server di aggiornamento di BitDefender e verificherà la disponibilità. Se viene rilevato un aggiornamento, secondo le opzioni impostate nella sezione Impostazioni Aggiornamento Manuale, vi verrà chiesto di confermarlo oppure verrà eseguito automaticamente.

Importante
Potrebbe essere necessario riavviare il computer una volta completato l'aggiornamento. Vi consigliamo di farlo appena possibile.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento di BitDefender su richiesta dell'utente.

12.1.2. Disattivare Aggiornamento Automatico

Scegliendo di disattivare l'aggiornamento automatico, apparirà una finestra di avviso.

Disattivare Aggiornamento Automatico

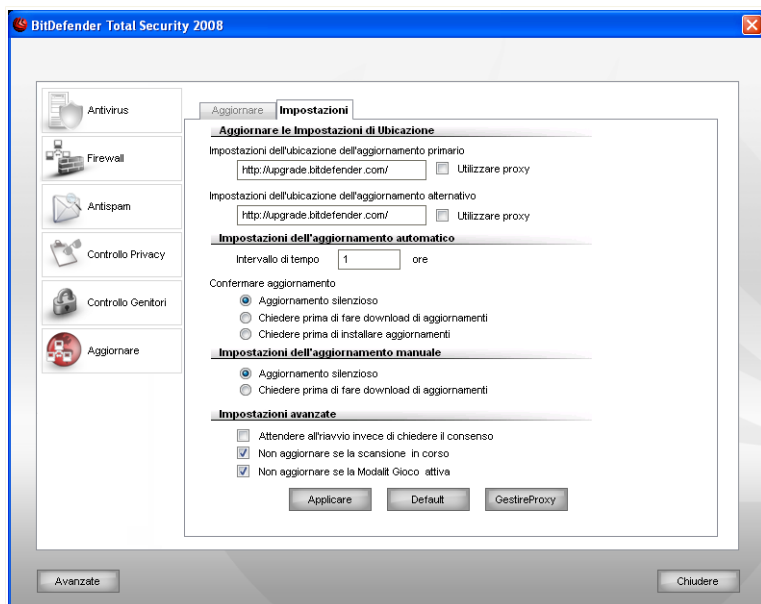
Dovete confermare la vostra scelta selezionando dal menu per quanto tempo volete che l'aggiornamentop automatico venga disattivato. Potete disattivare l'aggiornamento

automatico per 5, 15 o 30 minuti, per un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento
Questa è una questione critica di sicurezza. Vi consigliamo di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se BitDefender non verrà aggiornato regolarmente non sarà in grado di proteggervi dalle minacce più recenti.

12.2. Impostazioni dell’Aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy. Per default, BitDefender controllerà la disponibilità di aggiornamenti ogni ora sulla Internet ed installerà gli aggiornamenti disponibili senza avvisarvi.

Per configurare le impostazioni di aggiornamento e gestire i proxy, cliccare su **Aggiornamento>Impostazioni** nel console di configurazione. Apparirà la finestra seguente:

Impostazioni dell'Aggiornamento

Le impostazioni dell'aggiornamento sono ragruppate in 4 categorie (**Impostazioni Ubicazione Aggiornamento**, **Impostazioni Aggiornamento Automatico**, **Impostazioni Aggiornamento Manuale** ed **Impostazioni Avanzate**). Ogni categoria verrà descritta separatamente.

12.2.1. Impostare Ubicazioni Aggiornamento

Per configurare le ubicazioni dell'aggiornamento utilizzare le opzioni della categoria **Impostazioni Ubicazione Aggiornamento**.

Nota
Configurare queste impostazioni solo se siete connessi ad una rete locale che immagazzini localmente le impronte malware di BitDefender o se vi connettete ad Internet attraverso un server proxy.

Per aggiornamenti più affidabili e veloci, potete configurare due ubicazioni per l'aggiornamento: **Ubicazione principale dell'aggiornamento** e **Ubicazione**

alternativa dell'aggiornamento. Di default, queste ubicazioni sono la stessa:`http://upgrade.bitdefender.com`.

Per modificare una delle ubicazioni dell'aggiornamento, inserire l'URL dello specchio locale nel campo **URL** corrispondente all'ubicazione che si desidera modificare.

Nota
Vi consigliamo di impostare come ubicazione principale dell'aggiornamento lo specchio locale e di non modificare l'ubicazione alternativa, come piano di sicurezza interna nel caso in cui lo specchio locale non fosse disponibile.

Nel caso in cui l'azienda usi un server proxy per connettersi ad internet, selezionare **Usare proxy** e poi cliccare su **Gestione proxies** per configurare le impostazioni proxy.

Nota
Per ulteriori informazioni, vi preghiamo di riferirvi a «*Gestione Proxies*» (p. 199)

12.2.2. Configurazione Aggiornamento Automatico

Per configurare l'esecuzione automatica del processo di aggiornamento da parte di BitDefender, utilizzare le opzioni della categoria **Impostazioni Aggiornamento Automatico**.

Potete specificare il numero di ore tra due controlli consecutivi per aggiornamento nel campo **Intervallo di tempo**. Di default l'intervallo di tempo tra aggiornamenti è fissato in un'ora.

Per specificare come dovrebbe essere eseguito il processo di aggiornamento automatico, selezionare una delle seguenti opzioni:

- **Aggiornamento silenzioso** - BitDefender scarica ed implementa l'aggiornamento automaticamente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.

Nota
Vi verrà richiesto prima che gli aggiornamenti vengano scaricati anche se uscite dal Centro di Sicurezza.

- **Chiedere prima di installare gli aggiornamenti** - ogni volta che si scarica un aggiornamento, vi verrà richiesto se installarlo.

Nota

Vi verrà richiesto prima che gli aggiornamenti vengano installati anche se uscite dal Centro di Sicurezza.

12.2.3. Configurazione Aggiornamento Manuale

Per specificare come dovrà essere eseuito l'aggiornamento manuale (aggiornamento a richiesta dell'utente) selezionare una delle seguenti opzioni dalla categoria **Impostazioni Aggiornamento Manuali**:

- **Aggiornamento silenzioso** - l'aggiornamento manuale verrà eseguito automaticamente in background, senza l'intervento dell'utente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.

Nota

Vi verrà richiesto prima che gli aggiornamenti vengano scaricati anche se uscite dal Centro di Sicurezza.

12.2.4. Configurazione delle Impostazioni Avanzate

Per evitare che il processo di aggiornamento di BitDefender interferisca con il vostro lavoro, configurare le opzioni nella categoria **Impostazioni Avanzate**:

- **Attendi conferma prima di riavviare** - Se un aggiornamento richiede un riavvio, il prodotto continuerà a lavorare con i vecchi files fino a quando il sistema non sarà riavviato. Non verrà richiesto di riavviare il computer, per non interferire con il lavoro dell'utente.
- **Non aggiornare se la scansione è in corso** - BitDefender non verrà aggiornato se è in corso un processo di scansione. In questo modo la procedura di aggiornamento BitDefender non interferirà con le operazioni di scansione.

Nota

Se BitDefender viene aggiornato durante una scansione, la procedura di scansione sarà interrotta.

- **Non aggiornare se la modalità gioco è attiva** - BitDefender non eseguirà l'aggiornamento se la modalità gioco è attiva. In questo modo si può minimizzare l'influenza del prodotto sulla performance del vostro sistema durante i giochi.

12.2.5. Gestione Proxies

Se la vostra azienda utilizza un server proxy per connettersi ad Internet, dovrete specificare le impostazioni di proxy perchè BitDefender si possa aggiornare da solo. Altrimenti, esso utilizzerà le impostazioni proxy dell'amministratore che installò il prodotto o, se ci sono, le impostazioni predefinite del browser dell'utente corrente.

Nota
Le impostazioni del proxy possono essere configurate solo da utenti con diritti di amministratore sul computer oppure da "power users" (utenti che conoscono la password per le impostazioni del prodotto).

Per gestire le impostazioni del proxy, clicare su **Gestione proxies**. Apparirà la finestra **Gestore Proxy**.

Gestore Proxy

Vi sono tre gruppi di impostazioni del proxy:

- **Impostazioni del proxy dell'Amministratore (rilevate al momento dell'installazione)** - impostazioni del proxy rilevate sull'account dell'amministratore

durante l'installazione le quali possonoessere configurate solo utilizzando tale account. Se il server proxy richiede un nome utente ed una password, dovreste specificarli nei rispettivi campi.

- **Impostazioni del proxy dell'utente corrente (dal browser di default)** - Impostazioni del proxy dell'utente corrente, ricavate dal browser predefinito. Se il server proxy richiede un nome utente ed una password, dovreste specificarli nei rispettivi campi.

Nota
I browser web supportati sono Internet Explorer, Mozilla Firefox ed Opera. Se usate un altro browser di default, BitDefender non sarà in grado di ottenere le impostazioni del proxy dell'utente corrente.

- **Il vostro proprio set di impostazioni del proxy** - impostazioni del proxy che potrete configurare se vi siete registrati come amministratore.

  Le seguenti impostazioni devono essere spacificate:
  - **Indirizzo** - inserire l'IP del server proxy.
  - **Porta** - inserire la porta che utilizza BitDefender per connettersi al server proxy.
  - **Nome Utente** - inserire un nome utente riconosciuto dal proxy.
  - **Password** - inserire la password valida per l'utenza, già specificata precedentemente.

Quando ci si tenta di connettere ad Internet, ogni set di impostazione del proxy viene tentato uno alla volta, finchè BitDefender non riesce a connettersi.

In primo luogo verrà usato il set contenente le vostre impostazioni per connettersi ad Internet. Se questo non funzionasse, verranno utilizzate successivamente le impostazioni del proxy rilevate al momento dell'installazione. Ed infine, se neanche queste funzionassero, le impostazioni del proxy dell'utente corrente verranno ricavate dal browser predefinito ed utilizzate per connettersi ad Internet.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

Selezionare **Applica** per salvare le modifiche oppure **Default** per tornare alle impostazioni di default.

Amministrazione Avanzata del Backup

13. Amministrazione Avanzata del Backup

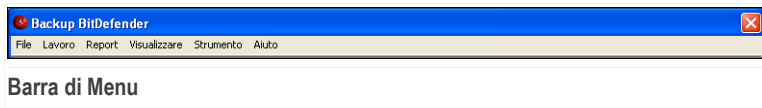
In questo capitolo vi verrà fornita una dettagliata introduzione alle caratteristiche del interfaccia graffico del Backup BitDefender.

Per iniziare a configurare le impostazioni del backup, cliccare semplicemente nella sezione **Backup** dell'area **Funzioni Veloci** e quindi cliccare su **Impostazioni Avanzate**.

Ci sono due modi in cui si possono impostare ed eseguire le operazioni di backup. Potete utilizzare la **Barra di Menu** nella parte superiore, o cliccare una certa sezione della **Barra di Navigazione**.

13.1. Barra di Menu

Ci sono sei menu disponibili per eseguire tutte le funzioni offerte dalla soluzione di backup di BitDefender.

Barra di Menu

File

- **Creare Nuovo Lavoro:** Mostra una finestra di dialogo per creare un nuovo lavoro di backup o un altro lavoro.
- **Aprire Set di Backup:** Mostra una finestra di dialogo per aprire il set di backup o il set di cataloghi per il recupero.
- **Uscire:** Consente di uscire dalla sezione di backup di BitDefender.

Lavoro

- **Backup:** Esegue il backup del lavoro selezionato. Se c'è più di un lavoro selezionato, eseguirà il backup di tutti i lavori selezionati.
- **Recuperare File:** Esegue il recupero del lavoro selezionato. Se c'è più di un lavoro selezionato, eseguirà il recupero di tutti i lavori selezionati.
- **Recuperare Dati di un Punto temporale:** Recupera il lavoro selezionato in un certo punto temporale. Se c'è più di un lavoro selezionato, eseguirà il recupero di tutti i file selezionati.
- **Programmazione:** Crea la programmazione del lavoro o modifica l'esistente.
- **Eliminare Programmazione:** Cancella la programmazione del lavoro specificato.

- **Eliminare:** Elimina il lavoro selezionato. Se c'è più di un lavoro selezionato, eseguirà l'eliminazione di tutti i file selezionati.
- **Eliminare tutti:** - cancella tutti i lavori nella Gestione lavori.
- **Sfoglia Destinazione:** Permette visualizzare i dati di backup della destinazione del lavoro selezionato.
- **Modificare Opzioni:** Modifica le opzioni del lavoro selezionato.
- **Proprietà:** Permette di modificare le proprietà del lavoro selezionato, inclusi dati in origine, nome, destinazione, etc del lavoro.

Report

- **Visualizzare Report:** Se il lavoro selezionato ha delle impostazioni di sicurezza, questa opzione vi permette di vedere i contenuti del report del lavoro.
- **Salvare come:** Salva i contenuti del report selezionato in un file specificato.
- **Stampare:** Stampa i contenuti del report selezionato .
- **Pulire tutto:** Cancella i contenuti del report del lavoro selezionato.
- **Aggiornare:** Aggiorna i contenuti del report del lavoro selezionato.

Visualizzare

- **Iniziare:** Se la finestra d'inizio non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Gestione Lavori:** Se la finestra Gestione Lavori non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Visualizzatore di Registro:** Se la finestra Visualizzatore di Registro non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Toolbox:** Se la finestra non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Mostrare Barra di Menu:** Nasconde la Barra di Menu. Per mostrarla, premere semplicemente **ALT**.
- **Mostrare Griglia:** Mostra o nasconde la griglia. Riguarda le finestre del visualizzatore di registro e della gestione lavori.

Strumento

- **Assistente di Backup:** Inizia la procedura di backup.
- **Assistente di Recupero:** Inizia la procedura di recupero.
- **Masterizzare:** avvia il masterizzatore CD/DVD/ISO o uno strumento di gestione di masterizzazione.
  - **Masterizzazione CD/DVD**
  - **Masterizzare File ISO**
  - **Visualizzare Infromazioni del Masterizzatore**
- **Esportare tutti i lavori:** Esporta tutti i lavori creati in un file specificato.
- **Importare Lavori:** Importa dei lavori da un file `.JOB`, `.TXT`, o `.XML`.
- **Esportare registri:** Esporta registri in un file `.TXT` o `.XML`.

- In un file `TXT`
- In un file `XML`

- **Importare registri:** Importa registri da un file `.TXT` o `.XML`.
  - Da un file `TXT`
  - Da un file `XML`
- **Opzioni:** Modifica le vostre opzioni globali di backup.
  - **Generale**
  - **Report e Registro**
  - **Programmazione Lavoro**

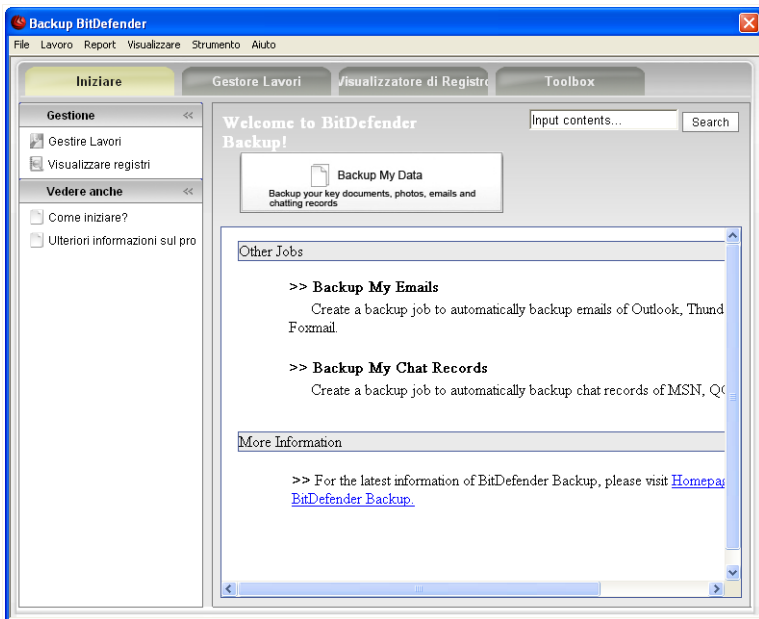
Aiuto

- **Argomento di Aiuto** - Mostra argomenti di aiuto.
- **Cercare:** Permette di cercare argomenti di aiuto in base alle parole chiavi selezionate o inserite.
- **BitDefender nella Pagina web:** Permette di accedere alla homepage di BitDefender per guardare le notizie su BitDefender ed il supporto on line.
- **Informazioni su Backup BitDefender:** Mostra le informazioni relative al copyright, la versione e l'edizione di Backup BitDefender.

13.2. Barra di Navigazione

La **Barra di Navigazione**, situata in alto nella finestra principale e sotto la **Barra di Menu**, da accesso a quattro sezioni:

- **Iniziare**
- **Gestione Lavori**
- **Visualizzatore di Registro**
- **Toolbox**

13.2.1. Iniziare

Iniziare

Potete procedere ad **Iniziare** faccendo come segue:

- Cliccare su **Iniziare** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barrra di Menu** e selezionare **Iniziare**.
- Utilizzare il collegamento premendo **CTRL+Alt+S**.

Per eseguire il backup dei vostri doumenti chiave, foto, mail e registri di chat durante lo stesso lavoro, cliccare sul tasto **Eseguire il Backup dei Miei Dati** e seguire la procedura di tre passi.

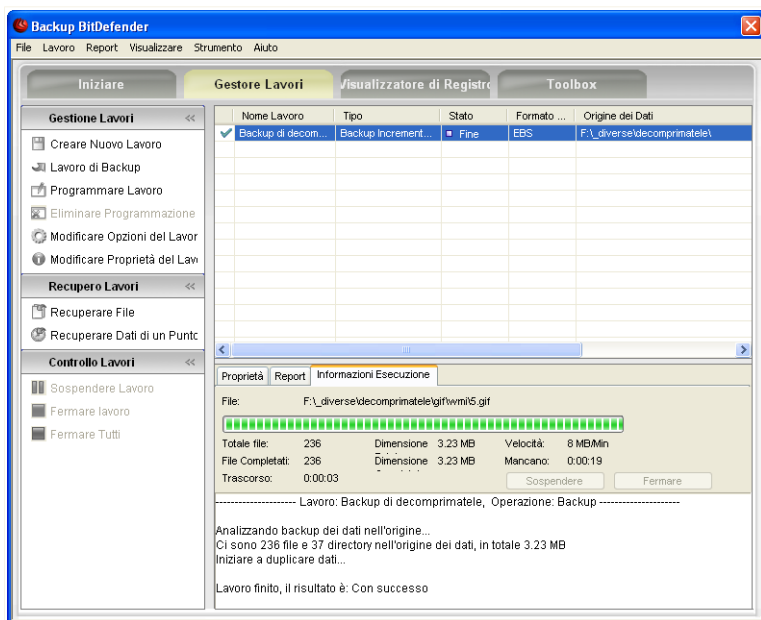
Per eseguire il backup solo delle vostre mail, cliccare sul tasto **Eseguire il Backup delle Mie Mail** e seguire la procedura di tre passi.

Per eseguire il backup solo dei vostri registri di chat, cliccare sul tasto **Eseguire il Backup dei Mei Registri di Chat** e seguire la procedura di tre passi.

Nota

La procedura di tre passi è anche descritta nella sezione Creare Nuovo Lavoro.

13.2.2. Gestione Lavori

La **Gestione Lavori** viene utilizzata per visualizzare e gestire i lavori di backup, visualizzare le proprietà ed i report dei lavori, così come per monitorare la velocità di esecuzione. **Gestione Lavori** permette anche di controllare le proprietà del lavoro e lo stato corrente, di modificare le sue impostazioni, così come di eseguire il backup o il recupero di esso.

Gestione Lavori

Potete passare a **Gestione Lavori** faccendo come segue:

- Cliccare su **Gestione Lavori** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barra di Menu** e selezionare **Gestione Lavori**.
- Utilizzare un collegamento, premendo **CTRL+Alt+M**.

Sulla sinistra, vedrete un elenco di links per operazioni veloci come segue:

Gestione Lavori

- **Creare Nuovo Lavoro**
- **Lavoro di Backup**
- **Lavoro programmato**
- **Eliminare Programmazione Lavoro**
- **Modificare Opzioni del Lavoro**
- **Modificare Proprietà del Lavoro**

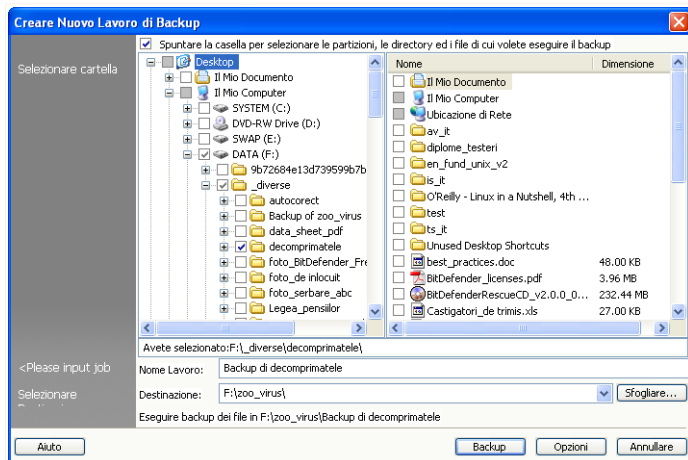
Recupero Lavoro

- **Recuperare File**
- **Recuperare Dati di un punto temporale**

Controllo Lavoro

- **Sospendere Lavoro**
- **Fermare Lavoro**
- **Fermare tutti**

Creare un Nuovo Lavoro

Per eseguire il backup dei vostri doumenti chiave, foto, mail e registri di chat durante lo stesso lavoro, cliccare sul tasto **Creare Nuovo Lavoro** e seguire questi tre passi.

Creare un Nuovo Lavoro

1. Cliccare nelle caselle per selezionare le partizioni, directory o file dei quali eseguire il backup.

   Quando selezionate un elemento nella parte sinistra della finestra, il suo contenuto verrà mostrato nella parte destra per aiutarvi a raffinare la vostra selezione.
2. Inserire un nome per il vostro lavoro di backup oppure accettare il nome lavoro predefinito.

   Quando i file o directory vengono selezionate per il backup, automaticamente si genera un nome lavoro predefinito, ma esso può essere modificato.
3. Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota
Non dimenticare di cliccare su **Backup** per iniziare oppure su **Cancellare** per fermare il lavoro.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Finestra di dialogo Opzioni di Backup

Ci sono diverse sotto-opzioni nella finestra **Opzioni**.

Finestra di dialogo Opzioni di Backup

Tipo di Backup

Backup BitDefender supporta due tipi di backup.

- **Backup completo:** Esegue il backup completo di tutti i dati in origine al set di backup verso la destinazione specificata, Quando si esegue il backup completo, Backup BitDefender non farà il backup solo dei dati modificati ma di tutto l'origine dei dati.
- **Backup Incrementale:** La prima volta che viene eseguito, il Backup incrementale è uguale al completo in quanto esegue il backup completo di tutti i dati in origine verso il set di backup nella destinazione specificata. Più tardi, esso salverà solo i file creati o modificati di recente. Ogni volta che viene eseguito un backup incrementale viene creato anche un set di cataloghi di backup.

I backup completo ed incrementale possono essere combinati in un **Backup a Rotazione**. Per esempio, potete impostare un backup incrementale del lavoro, mentre impostate un backup completo una volta a la settimana, diciamo la domenica. Verrebbe fatto così: Selezionare **Settimanalmente** nel menu a tendina, `1` nel campo **Ogni settimana** e selezionare Domenica. Questo Backup completo della domenica sostituirà tutti i backup precedenti e sarà la base dalla quale partirà il Backup incrementale.

Set di Cataloghi

Si utilizza per avere un indice dell'informazione sui file di ogni backup, edè la base del Backup incrementale e del processo di Recupero. Il set di cataloghi (`*.ecs`) contiene una serie di cataloghi che rappresentano un indice di tutti i file e directory nel set di backup. Tale indice include dati sulla data di backup, directory del backup, nome file e proprietà. I dati possono essere recuperati dal set di cataloghi.

Un nome file per il set di cataloghi viene generato automaticamente dalla destinazione del lavoro. Per modificare il set di cataloghi di un lavoro, fare come segue:

1. Cliccare su **Set di Cataloghi** .
2. Inserire il nome del file nel campo corrispondente.
3. Cliccare su **Sfoglia** per selezionare la directory dove salvare i file del Set di cataloghi.
4. Cliccare **OK**.

Compressione Dati

Backup BitDefender permette la compressione ed il salvataggio dei dati nel set di backup per il risparmio di spazio durante l'esecuzione del backup. Esso supporta la Compressione Veloce, Standard e la COmpressione ad Alta Intensità. Ad

esempio, per iniziare una compressione standard con grado e velocità di compressione medi, seguire questi passi:

1. Cliccare su **Compressione Dati**.
2. Cliccare su **Compressione Standard**.
3. Cliccare **OK**.

Ampiezza Destinazione

BitDefender Backup permette la distribuzione del set di backup su diverse destinazioni. In questo caso, anche se una certa destinazione non avrà sufficiente spazio libero, l'esecuzione del backup continuerà.

Potete aggiungere una o più destinazioni per continuare il backup, modificarle o addirittura rimuoverle, in uno dei seguenti modi:

1. Cliccare su **Ampiezza Destinazione**.
2. Cliccare su **Aggiungere** per selezionare una nuova destinazione dove salvare i dati del backup.
3. Cliccare su **Modificare** per modificare la destinazione di backup selezionata.
4. Cliccare su **Eliminare** per eliminare la destinazione di backup selezionata.
5. Cliccare su **Eliminare Tutte** per eliminare tutte le destinazioni di backup.
6. Cliccare **OK**.

Criptare

Backup BitDefender mantiene più sicuri i dati del backup criptando i dati prima di salvare il backup nel set. Le impostazioni di sicurezza di un lavoro includono la protezione mediante password.

Per criptare i dati prima del backup, seguire questi passi:

1. Cliccare su **Criptare**.
2. Scegliere un tipo di criptografia dal menu a tendina.
3. Inserire la vostra password nel campo corrispondente.
4. Reinserire la vostra password nel campo corrispondente.
5. Cliccare **OK**.

Programma Esterno

Il lavoro può eseguire altri comandi prima o dopo il backup, e il comando può essere `.exe`, `.com` o `.bat`, o un tipo specifico di evento come "spegnere il computer una volta completato il backup".

Per eseguire il comando all'inizio del backup, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Prima dell'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. Cliccare **OK**.

Per eseguire un comando dopo che il backup è terminato, seguire questi passi:
1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Dopo l'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. O cliccare su **Spegnere il computer** quando il backup sarà terminato.
5. O cliccare su **Riavviare il computer** quando il backup sarà terminato.
6. O cliccare su **Sconnettere l'utente corrente** quando il backup sarà terminato.
7. Cliccare **OK**.

Nota
Se volete che la configurazione lavori anche in caso di backup fallito, selezionare la casella **Eseguire Applicazione Esterna anche se l'Esecuzione del lavoro è fallita**.

Filtro File

Backup BitDefender fornisce una potente funzione di filtraggio per escludere o includere file, tipi di file o directory specificati, per risparmiare spazio disponibile e incrementare la velocità del backup.

I tipi di file specificati possono essere filtrati seguendo questi passi:
1. Cliccare su **Filtro File**.
2. Cliccare su **Tipo di Filtro**.
3. Escludere o includere i tipi di file nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i tipi di file selezionati** o **Escludere i tipi di file selezionati**.
4. Se necessario, inserire un altro tipo di file nel campo **Personalizzare tipo** ma assicuratevi di utilizzare il formato `.abc`. Usare `,` (virgola) come separatore quando inserite più di un tipo personalizzato. Aggiungere una breve descrizione nel campo corrispondente.
5. Cliccare **OK**.

I file specificati possono essere filtrati seguendo questi passi:
1. Cliccare su **Filtro File**.
2. Cliccare su **Filtro File**.
3. Escludere o includere i file specifici nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i file specificati dalla regola** o **Escludere i file specificati dalla regola**.
4. Cliccare su **Sfoglia** e selezionare il file. Il percorso all'ubicazione del file verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere il file non corrispondente alla sua ubicazione, cliccare su **Applicato a tutte le directory**.
5. Cliccare **OK**.

La directory specificata può essere filtrata seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtrare Directory**.
3. Escludere o includere directory specifiche nella finestra di dialogo che appare, selezionando le opzioni **Includere solo le directory specificate dalla regola** o **Escludere le directory specificate dalla regola**.
4. Cliccare su **Sfoglia** e selezionare la directory. Il percorso all'ubicazione della directory verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere directory non corrispondenti alle loro ubicazioni, cliccare su **Applicato a tutte le directory**.
5. Cliccare **OK**.

I filtri possono essere modificati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate modificare e quindi su **Modificare**.
3. Modificare le vostre opzioni nella finestra di dialogo.
4. Cliccare **OK**.

I filtri possono essere eliminati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate rimuovere e quindi su **Eliminare**.
3. O cliccare direttamente su **Eliminare Tutti**, per eliminare tutti i filtri.
4. Cliccare **OK**.

Trasferimento Rete

Backup BitDefender permette di eseguire accuratamente il backup ed il recupero di dati condivisi da gruppi di lavoro in rete. Se la rete non è accessibile riproverà ad effettuare il backup dei dati di volta in volta. per specificare la frequenza e quante volte riprovare a fare il backup, seguire questi passi.

1. Cliccare su**Trasferimento Rete**.
2. Cliccare su **In caso di mancata lettura di file in rete a causa di disconnessione, provare a riconnettere**.
3. Digitare la frequenza con cui volete ritentare il backup dei dati (in secondi).
4. Digitare quante volte ritentare il backup.
5. Cliccare **OK**.

Nota

Per evitare di essere travolti dalle informazioni su gli errori di rete, cliccare su **Nessun report di errore verrà generato quando la rete non è disponibile**.

Frazionamento del Set di Backup

Il set di backup generato può essere frazionato in molti altri set di backup, in modo che il backup possa essere eseguito normalmente anche quando la destinazione o file system sono limitati. Backup BitDefender fornisce due metodi di frazionamento: auto-split e sized-split.

Le impostazioni di frazionamento del backup del lavoro possono essere modificate come segue:

1. Cliccare su **Frazionamento del Set di Backup**.
2. Selezionare **Frazionamento Automatico in base allo Spazio nella Destinazione**.
3. O selezionare **Specificare la dimensione di frazionamento** e scegliere la dimensione desiderata dal menu a tendina.
4. Cliccare **OK**.

Velocità

Backup BitDefender supporta tre tipi di velocità. Più alta è la velocità, più CPU verrà utilizzata.

La velocità di Backup può essere specificata seguendo questi passi.

1. Cliccare su **Velocità**
2. Selezionare velocità **Massima**, **Media** o **Minima**.
3. Cliccare **OK**.

Verifica Dati

Per assicurarsi che i dati del vostro backup siano sempre sicuri, seguire questi passi.

1. Cliccare su **Verifica Dati**.
2. Cliccare su **Verificare i dati durante il processo di backup**.
3. Cliccare **OK**.

Lavoro di Backup

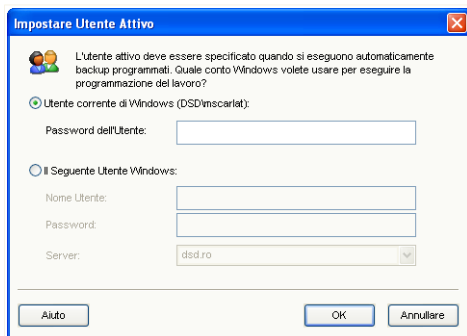
Una volta che il lavoro è stato creato il backup viene automaticamente eseguito. Tuttavia, potete accedere a **Gestione Lavori** per eseguire il backup selezionando il lavoro creato e cliccando su **Lavoro di Backup** nel menu.

Per ricevere i dettagli del backup durante il recupero dei file, dovete inserire una breve descrizione nel pop-up che si apre. Cliccare su **Annullare** per ignorare il pop-up oppure **OK** per continuare. Il lavoro di backup può essere anche cancellato cliccando sul tasto **Cancellare Backup**.

Nota

Per informazioni dettagliate, una buona idea sarebbe vedere **Proprietà**, **Report** e **Informazione su Esecuzione** del lavoro dalla finestra della barra di stato.

Programmare Lavoro

Qua potete programmare il lavoro di backup nel momentop più oppurtuno.Potete programmare il lavoro affinchè sia eseguito giornalmente, settimanalmente, mensilmente o in qualsiasi momento specificato (per esmpio all'avvio del sistema). **Programmare lavoro** è la base del backup automatico.

Programmare Lavoro

Se il vostro computer è membro di una rete di dominio, saranno necessari una serie di passi extra per aggiungere un programmatore di lavoro.

1. selezionare il lavoro e quindi cliccare su **Programmare Lavoro**.
2. Apparirà la finestra di dialogo **Utente Attivo**. Se voi siete l'utente di dominio, vi preghiamo di inserire la password di dominio.
3. Altrimenti selezionare **Eseguire come il seguente utente di Windows**.
4. Inserire il nome utente, la password ed il nome del server di dominio.
5. Cliccare **OK**.

Una volta che avete che avete impostato l'utente attivo, Backup BitDefender mostrerà la finestra **Programmazione** in modo che potrete impostare un momento opportuno per eseguire il lavoro.

Qua potete specificare la frequenza con cui i compiti programmati verranno eseguiti: giornalmente, settimanalmente, mensilmente, una volta, all'avvio del sistema,

all'accesso, quando il computer è ozioso. Se il compito è programmato giornalmente, settimanalmente, mensilmente, o una sola volta, potete anche specificare la data/ora di inizio. Potete selezionare anche la frequenza con cui il compito programmato verrà eseguito (espresso in numero di giorni o settimane, il giorno del mese o la data). Un'altra possibile impostazione sarebbe la durata (in minuti) del periodo di ozio dopo il quale il compito programmato verrà iniziato.

E' anche possibile configurare programmazioni multiple per un compito, cliccando su **Mostrare programmazioni multiple**. Cliccando su **Avanzate** potete impostare optioni di programmazione addizionali. Per esempio, potete definire la data di inizio e di fine del compito.

Per raffinare la programmazione del lavoro, cliccare sul tasto **Impostazioni**. Ci sono tre sub-opzioni disponibili.

- **Funzione programmata completata**
  - Eliminare il compito se non è prrogrammato per essere eseguito di nuovo.

    Questa funzione è utile per i compiti programmati per essere eseguiti solo una volta.
  - Fermare il compito se è in fase di esecuzione da:

    Specificare dopo quanto tempo dal suo inizio, il compito dovrebbe essere fermato.
- **Tempi Morti**
  - Iniziare il compito solo se il computer è stato ozioso per almeno:

    Specificare quanto tempo (in minuti) deve trascorrere senza uso del mouse o della tastiera prima che inizi il compito programmato.
  - Se il computer non è stato ozioso per così tanto, riprovare fino a:

    Specificare per quanto tempo (in minuti) il compito dovrà continuare a controllare se il computer è ozioso.
  - Fermare il compito se il computer smette di essere ozioso.

    Specificare se il compito si dovrà fermare nel caso in cui voi iniziate ad usare il computer mentre esso è in esecuzione.
- **Gestione Alimentazione**
  - Non iniziare il lavoro se il computer è in funzionamento con le batterie.

    Specificare se si dovrebbe evitare di iniziare il compito nel caso in cui il vostro computer sia in funzionamento con le batterie. Selezionando questa casella potrete prolungare la vita delle vostre batterie.
  - Fermare il compito se inizia la modalità batteria.

    Specificare se il compito dovrebbe essere fermato nel caso in cui il vostro computer inizi a funzionare con le batterie.

- Riattivare il computer per eseguire questo compito.

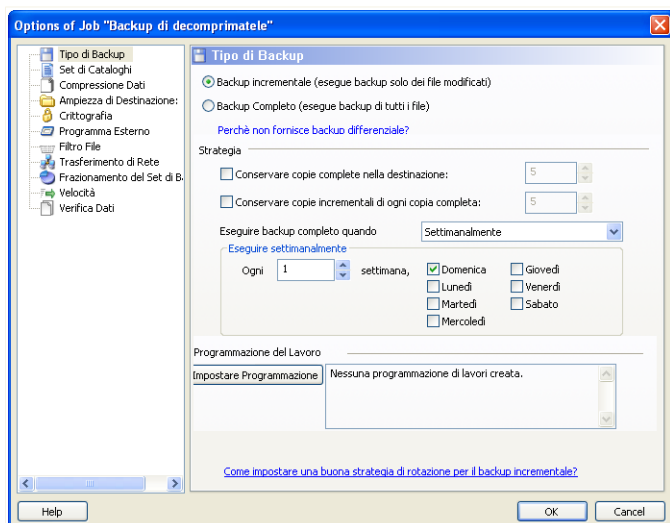
  Specificare se il computer dovrebbe eseguire il compito programmato anche quando è in sospensione.

Eliminare Programazione Lavoro

Per eliminare la programmazione di un lavoro, selezionarla e quindi cliccare su **Eliminare Programazione Lavoro** nella sezione **Gestione Lavori**.

Se il lavoro nonè stato programmato, **Eliminare Programazione Lavoro** verrà mostrato in grigio, il che significa che non è utilizzabile.

Modificare Opzioni Lavoro

Per modificare le opzioni di un lavoro, selezionarlo e quindi cliccare su **Modificare Opzioni Lavoro** nella sezione **Gestione Lavori**.

Modificare Opzioni Lavoro

Il lavoro selezionato può essere un lavoro di backup oppure di masterizzazione. Vediamoli uno alla volta.

Finestra di dialogo Opzioni di Backup

Ci sono diverse sotto-opzioni nella finestra **Opzioni**.

Finestra di dialogo Opzioni di Backup

Tipo di Backup

Backup BitDefender supporta due tipi di backup.

- **Backup completo:** Esegue il backup completo di tutti i dati in origine al set di backup verso la destinazione specificata, Quando si esegue il backup completo, Backup BitDefender non farà il backup solo dei dati modificati ma di tutto l'origine dei dati.
- **Backup Incrementale:** La prima volta che viene eseguito, il Backup incrementale è uguale al completo in quanto esegue il backup completo di tutti i dati in origine verso il set di backup nella destinazione specificata. Più tardi, esso salverà solo i file creati o modificati di recente. Ogni volta che viene eseguito un backup incrementale viene creato anche un set di cataloghi di backup.

I backup completo ed incrementale possono essere combinati in un **Backup a Rotazione**. Per esempio, potete impostare un backup incrementale del lavoro, mentre impostate un backup completo una volta a la settimana, diciamo la

domenica. Verrebbe fatto così: Selezionare **Settimanalmente** nel menu a tendina, `1` nel campo **Ogni settimana** e selezionare Domenica. Questo Backup completo della domenica sostituirà tutti i backup precedenti e sarà la base dalla quale partirà il Backup incrementale.

Set di Cataloghi

Si utilizza per avere un indice dell'informazione sui file di ogni backup, edè la base del Backup incrementale e del processo di Recupero. Il set di cataloghi (`*.ecs`) contiene una serie di cataloghi che rappresentano un indice di tutti i file e directory nel set di backup. Tale indice include dati sulla data di backup, directory del backup, nome file e proprietà. I dati possono essere recuperati dal set di cataloghi.

Un nome file per il set di cataloghi viene generato automaticamente dalla destinazione del lavoro. Per modificare il set di cataloghi di un lavoro, fare come segue:

1. Cliccare su **Set di Cataloghi** .
2. Inserire il nome del file nel campo corrispondente.
3. Cliccare su **Sfoglia** per selezionare la directory dove salvare i file del Set di cataloghi.
4. Cliccare **OK**.

Compressione Dati

Backup BitDefender permette la compressione ed il salvataggio dei dati nel set di backup per il risparmio di spazio durante l'esecuzione del backup. Esso supporta la Compressione Veloce, Standard e la COmpressione ad Alta Intensità. Ad esempio, per iniziare una compressione standard con grado e velocità di compressione medi, seguire questi passi:

1. Cliccare su **Compressione Dati**.
2. Cliccare su **Compressione Standard**.
3. Cliccare **OK**.

Ampiezza Destinazione

BitDefender Backup permette la distribuzione del set di backup su diverse destinazioni. In questo caso, anche se una certa destinazione non avrà sufficiente spazio libero, l'esecuzione del backup continuerà.

Potete aggiungere una o più destinazioni per continuare il backup, modificarle o addirittura rimuoverle, in uno dei seguenti modi:

1. Cliccare su **Ampiezza Destinazione**.
2. Cliccare su **Aggiungere** per selezionare una nuova destinazione dove salvare i dati del backup.
3. Cliccare su **Modificare** per modificare la destinazione di backup selezionata.

4. Cliccare su **Eliminare** per eliminare la destinazione di backup selezionata.
5. Cliccare su **Eliminare Tutte** per eliminare tutte le destinazioni di backup.
6. Cliccare **OK**.

Criptare

Backup BitDefender mantiene più sicuri i dati del backup criptando i dati prima di salvare il backup nel set. Le impostazioni di sicurezza di un lavoro includono la protezione mediante password.

Per criptare i dati prima del backup, seguire questi passi:

1. Cliccare su **Criptare**.
2. Scegliere un tipo di criptografia dal menu a tendina.
3. Inserire la vostra password nel campo corrispondente.
4. Reinserire la vostra password nel campo corrispondente.
5. Cliccare **OK**.

Programma Esterno

Il lavoro può eseguire altri comandi prima o dopo il backup, e il comando può essere `.exe`, `.com` o `.bat`, o un tipo specifico di evento come "spegnere il computer una volta completato il backup".

Per eseguire il comando all'inizio del backup, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Prima dell'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. Cliccare **OK**.

Per eseguire un comando dopo che il backup è terminato, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Dopo l'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. O cliccare su **Spegnere il computer** quando il backup sarà terminato.
5. O cliccare su **Riavviare il computer** quando il backup sarà terminato.
6. O cliccare su **Sconnettere l'utente corrente** quando il backup sarà terminato.
7. Cliccare **OK**.

Nota

Se volete che la configurazione lavori anche in caso di backup fallito, selezionare la casella **Eseguire Applicazione Esterna anche se l'Esecuzione del lavoro è fallita**.

Filtro File

Backup BitDefender fornisce una potente funzione di filtraggio per escludere o includere file, tipi di file o directory specificati, per risparmiare spazio disponibile e incrementare la velocità del backup.

I tipi di file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Tipo di Filtro**.
3. Escludere o includere i tipi di file nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i tipi di file selezionati** o **Escludere i tipi di file selezionati**.
4. Se necessario, inserire un altro tipo di file nel campo **Personalizzare tipo** ma assicuratevi di utilizzare il formato `.abc`. Usare `,` (virgola) come separatore quando inserite più di un tipo personalizzato. Aggiungere una breve descrizione nel campo corrispondente.
5. Cliccare **OK**.

I file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtro File**.
3. Escludere o includere i file specifici nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i file specificati dalla regola** o **Escludere i file specificati dalla regola**.
4. Cliccare su **Sfoglia** e selezionare il file. Il percorso all'ubicazione del file verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere il file non corrispondente alla sua ubicazione, cliccare su **Applicato a tutte le directory**.
5. Cliccare **OK**.

La directory specificata può essere filtrata seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtrare Directory**.
3. Escludere o includere directory specifiche nella finestra di dialogo che appare, selezionando le opzioni **Includere solo le directory specificate dalla regola** o **Escludere le directory specificate dalla regola**.
4. Cliccare su **Sfoglia** e selezionare la directory. Il percorso all'ubicazione della directory verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere directory non corrispondenti alle loro ubicazioni, cliccare su **Applicato a tutte le directory**.
5. Cliccare **OK**.

I filtri possono essere modificati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate modificare e quindi su **Modificare**.
3. Modificare le vostre opzioni nella finestra di dialogo.
4. Cliccare **OK**.

I filtri possono essere eliminati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate rimuovere e quindi su **Eliminare**.
3. O cliccare direttamente su **Eliminare Tutti**, per eliminare tutti i filtri.
4. Cliccare **OK**.

Trasferimento Rete

Backup BitDefender permette di eseguire accuratamente il backup ed il recupero di dati condivisi da gruppi di lavoro in rete. Se la rete non è accessibile riproverà ad effettuare il backup dei dati di volta in volta. per specificare la frequenza e quante volte riprovare a fare il backup, seguire questi passi.

1. Cliccare su**Trasferimento Rete**.
2. Cliccare su **In caso di mancata lettura di file in rete a causa di disconnessione, provare a riconnettere**.
3. Digitare la frequenza con cui volete ritentare il backup dei dati (in secondi).
4. Digitare quante volte ritentare il backup.
5. Cliccare **OK**.

Nota

Per evitare di essere travolti dalle informazioni su gli errori di rete, cliccare su **Nessun report di errore verrà generato quando la rete non è disponibile**.

Frazionamento del Set di Backup

Il set di backup generato può essere frazionato in molti altri set di backup, in modo che il backup possa essere eseguito normalmente anche quando la destinazione o file system sono limitati. Backup BitDefender fornisce due metodi di frazionamento: auto-split e sized-split.

Le impostazioni di frazionamento del backup del lavoro possono essere modificate come segue:

1. Cliccare su **Frazionamento del Set di Backup**.
2. Selezionare **Frazionamento Automatico in base allo Spazio nella Destinazione**.
3. O selezionare **Specificare la dimensione di frazionamento** e scegliere la dimensione desiderata dal menu a tendina.
4. Cliccare **OK**.

Velocità

Backup BitDefender supporta tre tipi di velocità. Più alta è la velocità, più CPU verrà utilizzata.

La velocità di Backup può essere specificata seguendo questi passi.

1. Cliccare su **Velocità**
2. Selezionare velocità **Massima**, **Media** o **Minima**.
3. Cliccare **OK**.

Verifica Dati

Per assicurarsi che i dati del vostro backup siano sempre sicuri, seguire questi passi.

1. Cliccare su **Verifica Dati**.
2. Cliccare su **Verificare i dati durante il processo di backup**.
3. Cliccare **OK**.

Modificare le Opzioni di un Lavoro di Masterizzazione

Ci sono diverse sub-opzioni disponibili nella finestra di dialogo del lavoro di masterizzazione.

Masterizzazione

Qua potete impostare se il disco deve essere espellito dopo la masterizzazione, finalizzato (se programmate di condividerlo con gli altri) oppure scritto usando il Joliet file system (meno restrizioni del nome file).

Se volete programmare il lavoro, cliccare su **Impostare Programmazione**.

Qua potete programmare il lavoro di backup nel momentop più oppurtuno.Potete programmare il lavoro affinchè sia eseguito giornalmente, settimanalmente, mensilmente o in qualsiasi momento specificato (per esmpio all'avvio del sistema). **Programmare lavoro** è la base del backup automatico.

Se il vostro computer è membro di una rete di dominio, saranno necessari una serie di passi extra per aggiungere un programmatore di lavoro.

1. selezionare il lavoro e quindi cliccare su **Programmare Lavoro**.
2. Apparirà la finestra di dialogo **Utente Attivo**. Se voi siete l'utente di dominio, vi preghiamo di inserire la password di dominio.
3. Altrimenti selezionare **Eseguire come il seguente utente di Windows**.
4. Inserire il nome utente, la password ed il nome del server di dominio.
5. Cliccare **OK**.

Una volta che avete che avete impostato l'utente attivo, Backup BitDefender mostrerà la finestra **Programmazione** in modo che potrete impostare un momento opportuno per eseguire il lavoro.

Qua potete specificare la frequenza con cui i compiti programmati verranno eseguiti: giornalmente, settimanalmente, mensilmente, una volta, all'avvio del sistema, all'accesso, quando il computer è ozioso. Se il compito è programmato giornalmente, settimanalmente, mensilmente, o una sola volta, potete anche specificare la data/ora di inizio. Potete selezionare anche la frequenza con cui il compito programmato verrà eseguito (espresso in numero di giorni o settimane, il giorno del mese o la data). Un'altra possibile impostazione sarebbe la durata (in minuti) del periodo di ozio dopo il quale il compito programmato verrà iniziato.

E' anche possibile configurare programmazioni multiple per un compito, cliccando su **Mostrare programmazioni multiple**. Cliccando su **Avanzate** potete impostare optioni di programmazione addizionali. Per esempio, potete definire la data di inizio e di fine del compito.

Per raffinare la programmazione del lavoro, cliccare sul tasto **Impostazioni**. Ci sono tre sub-opzioni disponibili.

- **Funzione programmata completata**
  - Eliminare il compito se non è prrogrammato per essere eseguito di nuovo.

    Questa funzione è utile per i compiti programmati per essere eseguiti solo una volta.
  - Fermare il compito se è in fase di esecuzione da:

    Specificare dopo quanto tempo dal suo inizio, il compito dovrebbe essere fermato.
- **Tempi Morti**
  - Iniziare il compito solo se il computer è stato ozioso per almeno:

    Specificare quanto tempo (in minuti) deve trascorrere senza uso del mouse o della tastiera prima che inizi il compito programmato.
  - Se il computer non è stato ozioso per così tanto, riprovare fino a:

    Specificare per quanto tempo (in minuti) il compito dovrà continuare a controllare se il computer è ozioso.
  - Fermare il compito se il computer smette di essere ozioso.

    Specificare se il compito si dovrà fermare nel caso in cui voi iniziate ad usare il computer mentre esso è in esecuzione.
- **Gestione Alimentazione**
  - Non iniziare il lavoro se il computer è in funzionamento con le batterie.

Specificare se si dovrebbe evitare di iniziare il compito nel caso in cui il vostro computer sia in funzionamento con le batterie. Selezionando questa casella potrete prolungare la vita delle vostre batterie.

- Fermare il compito se inizia la modalità batteria.

  Specificare se il compito dovrebbe essere fermato nel caso in cui il vostro computer inizi a funzionare con le batterie.

- Riattivare il computer per eseguire questo compito.

  Specificare se il computer dovrebbe eseguire il compito programmato anche quando è in sospensione.

Programma Esterno

Il lavoro può eseguire altri comandi prima o dopo il backup, e il comando può essere `.exe`, `.com` o `.bat`, o un tipo specifico di evento come "spegnere il computer una volta completato il backup".

Per eseguire il comando all'inizio del backup, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Prima dell'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. Cliccare **OK**.

Per eseguire un comando dopo che il backup è terminato, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Dopo l'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. O cliccare su **Spegnere il computer** quando il backup sarà terminato.
5. O cliccare su **Riavviare il computer** quando il backup sarà terminato.
6. O cliccare su **Sconnettere l'utente corrente** quando il backup sarà terminato.
7. Cliccare **OK**.

Nota

Se volete che la configurazione lavori anche in caso di backup fallito, selezionare la casella **Eseguire Applicazione Esterna anche se l'Esecuzione del lavoro è fallita**.

Filtro File

Backup BitDefender fornisce una potente funzione di filtraggio per escludere o includere file, tipi di file o directory specificati, per risparmiare spazio disponibile e incrementare la velocità del backup.

I tipi di file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.

2. Cliccare su **Tipo di Filtro**.
3. Escludere o includere i tipi di file nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i tipi di file selezionati** o **Escludere i tipi di file selezionati**.
4. Se necessario, inserire un altro tipo di file nel campo **Personalizzare tipo** ma assicuratevi di utilizzare il formato `.abc`. Usare `,` (virgola) come separatore quando inserite più di un tipo personalizzato. Aggiungere una breve descrizione nel campo corrispondente.
5. Cliccare **OK**.

I file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtro File**.
3. Escludere o includere i file specifici nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i file specificati dalla regola** o **Escludere i file specificati dalla regola**.
4. Cliccare su **Sfoglia** e selezionare il file. Il percorso all'ubicazione del file verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere il file non corrispondente alla sua ubicazione, cliccare su **Applicato a tutte le directory**.
5. Cliccare **OK**.

La directory specificata può essere filtrata seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtrare Directory**.
3. Escludere o includere directory specifiche nella finestra di dialogo che appare, selezionando le opzioni **Includere solo le directory specificate dalla regola** o **Escludere le directory specificate dalla regola**.
4. Cliccare su **Sfoglia** e selezionare la directory. Il percorso all'ubicazione della directory verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere directory non corrispondenti alle loro ubicazioni, cliccare su **Applicato a tutte le directory**.
5. Cliccare **OK**.

I filtri possono essere modificati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate modificare e quindi su **Modificare**.
3. Modificare le vostre opzioni nella finestra di dialogo.
4. Cliccare **OK**.

I filtri possono essere eliminati seguendo questi passi:

1. Cliccare su **Filtro File**.

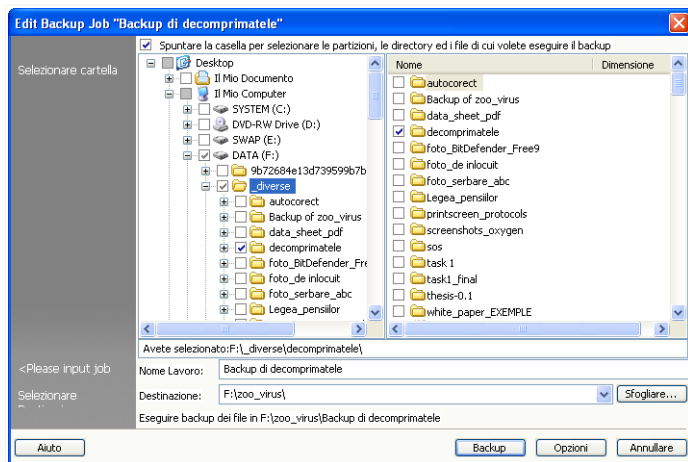
2. Cliccare sul filtro che desiderate rimuovere e quindi su **Eliminare**.
3. O cliccare direttamente su **Eliminare Tutti**, per eliminare tutti i filtri.
4. Cliccare **OK**.

Verifica Dati

Per assicurarsi che i dati del vostro backup siano sempre sicuri, seguire questi passi.

1. Cliccare su **Verifica Dati**.
2. Cliccare su **Verificare i dati durante il processo di backup**.
3. Cliccare **OK**.

Modificare Proprietà del Lavoro

Per modificare le proprietà di un lavoro, selezionare il lavoro interessato e quindi cliccare **Modificare Proprietà del Lavoro** nella sezione **Gestione Lavori**.

Modificare Proprietà del Lavoro

1. Cliccare nelle caselle per selezionare le partizioni, directory o file dei quali eseguire il backup.

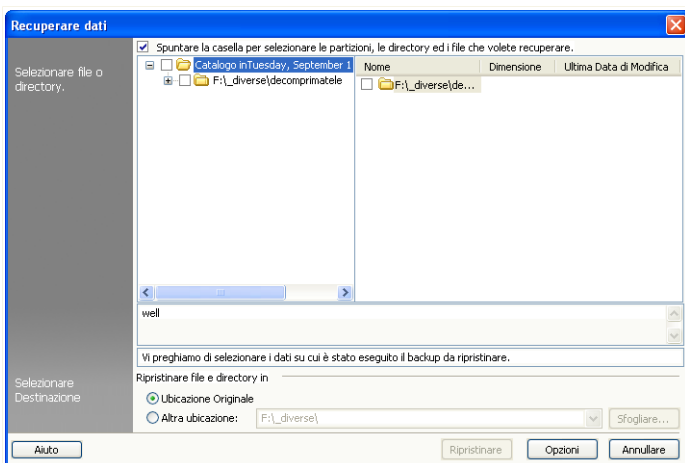
   Quando selezionate un elemento nella parte sinistra della finestra, il suo contenuto verrà mostrato nella parte destra per aiutarvi a raffinare la vostra selezione.
2. Inserire un nome per il vostro lavoro di backup oppure accettare il nome lavoro predefinito.

Quando i file o directory vengono selezionate per il backup, automaticamente si genera un nome lavoro predefinito, ma esso può essere modificato.

3. Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota
Non dimenticare di cliccare su **Backup** per iniziare oppure su **Cancellare** per fermare il lavoro.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Recuperare File

Per recuperare i vostri dati dal backup, selezionare il lavoro dal quale volete recuperare i dati, cliccare su **Recuperare File** nel menu **Recupero Lavori** e quindi seguire questi passi.

Recuperare File

1. Selezionare le caselle accanto alle partizioni, directory o file da recuperare.

   Quando selezionate un elemento nella parte sinistra della finestra, il suo contenuto verrà mostrato nella parte destra per aiutarvia raffinare la selezione.

2. Nella finestra **Selezionare Ubicazione di Recupero**, potete usare l'ubicazione originale senza nessun cambio oppure specificare un'altra ubicazione dove ripristinare il file.

Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota
Non dimenticare di cliccare su **Recuperare** per iniziare oppure **Cancellarel** per fermare il processo.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Finestra di dialogo delle Opzioni di Recupero

Le opzioni di recupero permettono di specificare se i file da ripristinare esistono già nella destinazione nel momento del recupero, e se aggiornare la data di modifica di ogni file ripristinato.

Quando i file da ripristinare esistono già

- **Ignorare File** BitDefender ignora i relativi file.
- **Chiedere all'utente** BitDefender vi chiede se sostituire o meno i file già esistenti.
- **Sostituzione Diretta** BitDefender sostituisce i file senza chiedere il consenso.
- **Sostituire i più vecchi** BitDefender sostituisce solo i file più vecchi, I file più vecchi vengono determinati dalla data in cui sono stati modificati.

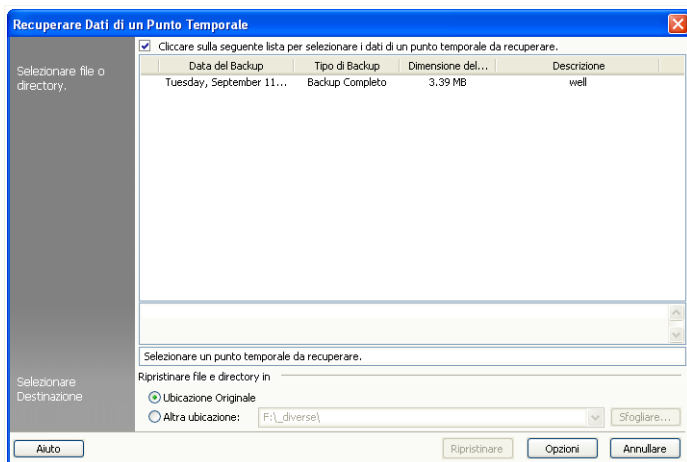
Data di Modifica del File

Se l'opzione è selezionata, BitDefender utilizza la data corrente per indicare la data in cui i file e directory sono stati ripristinati. Se non, BitDefender utilizzerà come data di modifica del file o directory quella in cui è stato eseguito il backup.

Struttura della Directory

Diventa attiva solo se scegliete di ripristinare i dati in un'altra directory. Potete anche conservare la struttura di directory dei vostri dati.

Recuperare dati di un punto temporale

Per ripristinare i dati su cui avete eseguito il backup in un punto temporale specifico, selezionare il lavoro dal quale volete recuperare i dati, cliccare su **Recuperare dati di un punto temporale** nel menu **Recupero Lavoro** e quindi seguire questi passi.

Recuperare dati di un punto temporale

1. Selezionare dalla lista il set di backup di un punto temporale specificato. I commenti verranno mostrati sotto.
2. Nella finestra **Selezionare Ubicazione di Recupero**, potete usare l'ubicazione originale, senza modifiche, o specificare un'altra ubicazione dove ripristinare il file.

   Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota
Non dimenticare di cliccare su **Recuperare** per iniziare oppure **Cancellarel** per fermare il processo.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Finestra di dialogo delle Opzioni di Recupero

Le opzioni di recupero permettono di specificare se i file da ripristinare esistono già nella destinazione nel momento del recupero, e se aggiornare la data di modifica di ogni file ripristinato.

Quando i file da ripristinare esistono già

- **Sostituire i più vecchi** BitDefender sostituisce solo i file più vecchi, I file più vecchi vengono determinati dalla data in cui sono stati modificati.

Data di Modifica del File
Se l'opzione è selezionata, BitDefender utilizza la data corrente per indicare la data in cui i file e directory sono stati ripristinati. Se non, BitDefender utilizzerà come data di modifica del file o directory quella in cui è stato eseguito il backup.

Struttura della Directory
Diventa attiva solo se scegliete di ripristinare i dati in un'altra directory. Potete anche conservare la struttura di directory dei vostri dati.

Controllo Lavori

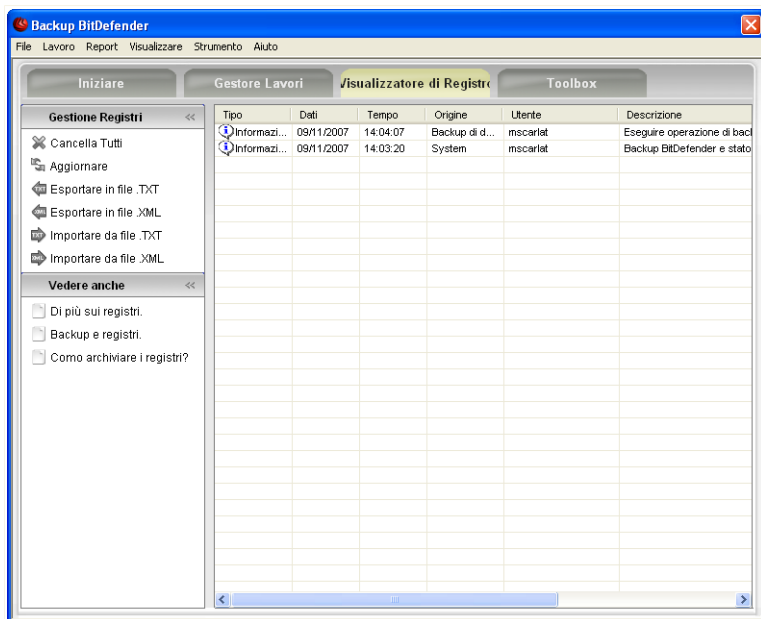
Ci sono tre modi di controllare un lavoro: sospendere, fermare e fermare tutti.

Pausa
Per sospendere un lavoro di backup o di recupero in corso, cliccare sul tasto **Sospendere Lavoro** nel menu **Controllo Lavori**.

Fermare
Per fermare un lavoro di backup o di recupero in corso, cliccare sul tasto **Fermare Lavoro** nel menu **Controllo Lavori**.

Fermare tutti
Se ci sono più di un lavoro di backup o di recupero in corso, non c'è bisogno di fermarli uno per uno. Cliccare sul tasto **Fermare Tutti** nel menu **Controllo Lavori** per fermarli tutti in una volta sola.

13.2.3. Visualizzatore di Registro

Questa sezione vi mostra come visualizzare, importare, esportare e cancellare i registri. L'opzione Registro vi permette di ricordare quello che avete salvato mediante backup e recuperato e quando lo avete fatto, e vi mostra anche gli avvisi o gli errori nelle operazioni. Per esempio, se si verifica un errore di lettura di un file durante l'esecuzione, BitDefenser lo registrerà come un messaggio di avviso.

Visualizzatore di Registro

Potete passare a **Visualizzatore di Registro** faccendo come segue:

- Cliccare su **Visualizzatore di Registro** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barra di Menu** e selezionare **Visualizzatore di Registro**.
- Utilizzare un collegamento premendo **CTRL+Alt+L**.

Visualizzare Registri

L'opzione di visualizzazione dei registri vi permette di rintracciare la vostra operazione e scoprire la causa dell'errore nell'operazione.

La descrizione di un registro in Backup BitDefender contiene i seguenti elementi:

Tipo

Una classifica della severità del registro. Ci sono quattro gradi di severità in Backup BitDefender:

- **Fatale:** Un problema significativo che impedisce a Backup BitDefender di funzionare normalmente. Per esempio, il file di configurazione di Backup BitDefender è stato danneggiato.
- **Errore:** Un problema che conduce al fallimento di un'operazione. Per esempio, è stato eseguito il backup di un lavoro su un server, ma il server è inaccessibile.
- **Avviso:** un problema che non colpisce un'operazione, ma può essere classificato più tardi come evento. Per esempio, un file non può essere letto nel processo di backup.
- **Informazione:** Descrive un'operazione eseguita con successo. Per esempio, un lavoro è stato eliminato con successo.

Data
La data in cui l'oggetto del registro è accaduto.

Ora
L'ora locale in cui l'oggetto del registro è accaduto.

Origine
L'origine del registro dell'oggetto, il quale può essere un lavoro oppure l'applicazione Backup BitDefender. Per esempio, un oggetto con il commento System indica che esso è stato generato dalla l'applicazione Backup BitDefender. Altri possibili commenti sono i nomi dei processi di Backup BitDefender che abbianno registrato i relativi elementi.

Utente
Il nome del utente la cui azione a generato il registro dell'oggetto.

Descrizione
Presenta il contenuto dettagliato dellìoggetto registrato.

Cancellare Registri

Backup BitDefender fornisce due modi per cancellare i registri: automaticamente e manualmente.

Importante
Una volta che il registro è stato cancellato, non può essere più recuperato. Per ciò, è meglio esportare tutti i registri in un file e conservarli per consultazioni future.

Cancellare Automaticamente
All'inizio di Backup BitDefender, appare la dimensione di registro esistente cone dimensione predefinita, Backup BitDefender cancellerà automaticamente tutti i file di registro che eccedano la dimensione predefinita.

Nota
Per scoprire o modificare la dimensione predefinita di registro, seguire questi passi:
1. Cliccare su **Strumenti** nella **Barra di Menu**.
2. Cliccare su **Opzioni** e quindi selezionare **Report e Registro**.
3. Inserire il limite di dimensione desiderato (in MB) nel campo corrispondente. Quando la dimensione del registro raggiungerà questo limite, Backup BitDefender cancellerà tutti i registri.

Cancellare Manualmente

Seguire questi passi per cancellare i registri manualmente.
1. Cliccare su **Cancella Tutti** nel menu **Gestione Registri**.
2. Cliccare **OK** per espotare certi registri prima di cancellare gli altri, o cliccare **No** se non volete conservare alcun registro.

Importare ed Esportare Registri

Backup BitDefender supporta attualmente l'importazione ed esportazione di file in due formati: `.TXT` e `.XML`

Nota
Vi consigliamo di esportare e salvare il registro in un file prima di cancellarlo.

Per esportare i registri in un file specifico, seguire questi passi:

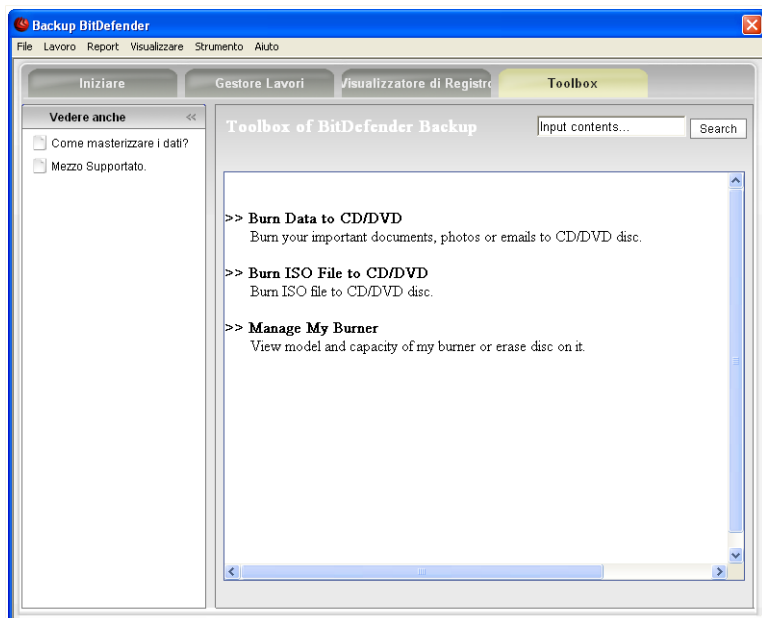
1. Cliccare **Esportare in file .TXT** o **Esportare in file .XML** nel menu **Gestione Registri**.
2. Inserire il nome file e scegliere l'ubicazione dove salvare il vostro file.
3. Cliccare su **Salvare**,

Per importare registri da un file specifico, seguire questi passi:

1. Cliccare su **Importare in file .TXT** o **Importare in file .XML** nel menu **Gestione Registri**.
2. Trovare il vostro File.
3. Cliccare **Aprire**.

Nota
Cliccare sul tasto **Aggiornare** nel menu **Gestione Registri** per assicurarvi che visualizzate i registri più recenti.

13.2.4. Toolbox

Questa sezione vi mostra come utilizzare Backup BitDefender per masterizzare dati su CD/DVD oppure masterizzare un file d'immagine ISO. Copre argomenti come la masterizzazione di CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL e la conservazione fuori rete dei dati resultanti del backup.

Toolbox

Petete passare alla **Toolbox** faccendo come segue:

- Cliccare su **Toolbox** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barra di Menu** e selezionare **Toolbox**.
- Utilizzare il collegamento premendo **CTRL+Alt+T**.

Masterizzare su CD/DVD

Per masterizzare dati su CD/DVD manualmente, seguire questi passi:

1. Cliccare su **masterizzare dati su CD/DVD** .
2. Cliccare su **Cancellare** se volete riutilizzare un disco riscrivibile. Se desiderate cancellarlo velocemente, cliccare su **Veloce**. Se avete bisogno di cancellare completamente l'informazione registrata, cliccare su **Completa**, ma questo richiederà un po' di tempo.
3. Cliccare su **Masterizzare con dialogo**.

   Qua potete impostare se il disco deve essere espellito dopo la masterizzazione, finalizzato (se programmate di condividerlo con gli altri) oppure scritto usando il Joliet file system (meno restrizioni del nome file).
4. Cliccare su **File** or**Directory** nella finestra di dialogo che appare per aggiungere dati che volete masterizzare.
5. Dopo che avete aggiunto i dati, selezionare il masterizzatore ed il nome del disco sul quale verranno masterizzati i dati, e quindi cliccare su **Masterizzare**.

Masterizzare File d'Immagine ISO su CD/DVD

Per masterizzare un file d'immagine ISO su CD/DVD, seguire questi passi:

1. Cliccare su **Masterizzare File d'Immagine ISO su CD/DVD**.
2. Cliccare su **Cancellare** se volete riutilizzare un disco riscrivibile. Se desiderate cancellarlo velocemente, cliccare su **Veloce**. Se avete bisogno di cancellare completamente l'informazione registrata, cliccare su **Completa**, ma questo richiederà un po' di tempo.
3. Cliccare su **Masterizzare con dialogo**.

   Qua potete impostare se il disco deve essere espellito dopo la masterizzazione, finalizzato (se programmate di condividerlo con gli altri) oppure scritto usando il sistema Joliet file (meno restrizioni del nome file).
4. Selezionare **Aggiungere**.
5. Scegliere un file d'immagine ISO da masterizzare e cliccare **OK**.
6. Cliccare su **Masterizzare**.

Gestione del Masterizzatore

Questo vi aiuta a gestire e visualizzare il dispositivo di registrazione ed i dischi nel sistema corrente. Contiene i seguenti links:

- **Eject** Apre il dispositivo di registrazione selezionato.
- **Chiudere** Chiude il dispositivo di registrazione selezionato.
- **Informazioni Media** Permette di visualizzare le informazioni Media del dispositivo di registrazione.

- **Inforamzioni Dispositivo** Permette di visualizzare le informazioni sul dispositivo di registrazione.
- **Potenzialità** Permette di visualizzare le potenzialità del dispositivo di registrazione.
- **Cancellare Media** Cancella i contenuti del disco.

BitDefender Rescue CD

14. Informazioni generali sul prodotto BitDefender™

Sicurezza Totale BitDefender 2008 arriva con un CD avviabile (BitDefender Rescue CD), in grado di eseguire la scansione e disinfettare tutti i dischi rigidi prima che parta il vostro Sistema Operativo.

Dovreste usare il Rescue CD ogni volta che il vostro sistema operativo non lavora correttamente per via di infezioni di virus. Generalmente accade quando non viene utilizzato un prodotto antivirus.

L'aggiornamento dell'impronta dei virus viene eseguita automaticamente, senza l'intervento dell'utente, ogni volta che si avvia il Rescue CD BitDefender.

BitDefender Rescue CD è una distribuzione di Knoppix ri-masterizzato di BitDefender, che integra l'ultima soluzione di sicurezza di BitDefender per Linux nel CD GNU/Linux Knoppix Live, offrendo un antivirus di desktop capace di eseguire la scansione e disinfettare tutti i dischi rigidi esistenti (includendo partizioni NTFS di Windows). Nello stesso tempo BitDefender Rescue CD può essere utilizzato per recuperare i vostri dati preziosi quando non si può avviare Windows

14.1. Requisiti del sistema

Prima di avviare BitDefender Rescue CD, dovete innanzitutto verificare se il vostro sistema ha i seguenti requisiti.

Tipo di processore
: Compatibile x86, minimo 166 MHz, ma non attendetevi un alto rendimento in questo caso. Un processore di generazione i686, a 800 MHz sarebbe una scelta migliore.

Memoria
: Minimo 512 MB di Memoria RAM (raccomandati 1 GB)

CD-ROM
: BitDefender Rescue CD si esegue da un CD-ROM, per cui sono richiesti un CD-ROM ed un BIOS in grado di avviarlo.

Connessione Internet
: Anche se BitDefender Rescue CD funzionerà senza connessione alla rete, le procedure di aggiornamento richiederanno un link HTTP attivo, persino attraverso

alcuni server proxy. Di conseguenza, per una protezione aggiornata, la connessione ad Internet è obbligatoria.

Risoluzione grafica
Scheda grafica standard SVGA-compatibile.

14.2. Software Incluso

Il BitDefender Rescue CD include i seguenti pacchetti software.

Xedit
Questo è un editore di file di testo.

Vim
Questo è un potente editore di file di testo, contenente evidenziatore di sintassi, un GUI, e molto altro.Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Vim.

Xcalc
Questa è una calcolatrice.

RoxFiler
RoxFiler è un veloce e potente gestore di file grafici.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) è un gestore di file text-mode.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di MC .

Pstree
Pstree mostra i processi in corso.

Top
Top mostra le funzioni Linux.

Xkill
Xkill blocca tutte le X risorse di un client.

Partition Image
Partition Image vi aiuta a salvare le partizioni nei formati dei file di sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 in un file di immagine. Questo programma può essere utile a fini di backup.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Partimage.

GtkRecover

GtkRecover è una versione GTK del console del programma di recupero. Aiuta a recuperare dei file.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di GtkRecover.

ChkRootKit

ChkRootKit è uno strumento che vi aiuta ad effettuare la scansione del vostro computer in cerca di rootkits.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di ChkRootKit.

Nessus Network Scanner

Nessus è uno scanner di sicurezza remota per Linux, Solaris, FreeBSD, e Mac OS X.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di Nessus.

Iptraf

Iptraf è un Software di monitoraggio di rete IP.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Iptraf.

Iftop

Iftop mostra l'uso di larghezza di banda su di un interfaccia.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Iftop.

MTR

MTR è uno strumento di diagnosi di rete.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di MTR .

PPPStatus

PPPStatus mostra le statistiche sul traffico TCP/IP in entrata ed in uscita.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di PPPStatus.

Wavemon

Wavemon è un'applicazione di monitoraggio per dispositivi di rete wireless.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di Wavemon.

USBView

USBView mostra informazioni sui dispositivi connessi al bus USB.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di USBView.

Pppconfig

Pppconfig aiuta a configurare automaticamente una connessione dial up ppp.

DSL/PPPoe
DSL/PPPoe configura una connessione PPPoE (ADSL).

I810rotate
I810rotate cambia l'output su video a i810 hardware usando i810switch(1).

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di I810rotate .

Mutt
Mutt è un potente mail client MIME basato su testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Mutt.

Mozilla Firefox
Mozilla Firefox è un noto browser web.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Mozilla Firefox.

Elinks
Elinks browser di web in modo testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Elinks.

15. BitDefender Rescue CD fai-da-te.

Questo capitolo contiene informazioni su come iniziare e fermare il BitDefender Rescue CD, come eseguire la scansione del vostro computer alla ricerca di malware e anche come salvare dati dal vostro PC Windows compromesso su un dispositivo rimuovibile. In ogni caso, utilizzando le applicazioni software contenute nel CD, potrete eseguire molti processi, la cui descrizione va oltre gli obiettivi di questo manuale.

15.1. Avviare BitDefender Rescue CD

Per avviare il CD, configurare il BIOS del vostro computer per avviarlo dal CD, inserire il CD nel dreve e riavviare il computer. Assicurati che il vostro computer possa avviarsi dal CD.

Attendere che venga mostrata la finestra successiva e seguire le istruzioni per avviare BitDefender Rescue CD.

Boot Splash Screen

L’aggiornamento delle impronte dei virus è eseguita automaticamente. Questo potrebbe richiedere qualche istante.

Quando il processo di avvio è finito vedrete il successivo desktop. Adesso potete cominciare ad utilizzare il BitDefender Rescue CD.

Il Desktop

15.2. Arrestare BitDefender Rescue CD

Potete chiudere il vostro computer in modo sicuro selezionando **Uscire** dal menu contestuale di BitDefender Rescue CD (tasto destro per aprirlo) o usando il comando **Fermare** su un terminale.

Scegliere “Uscire”

Quando BitDefender Rescue CD avrà chiuso tutti i programmi con successo, mostrerà una schermata come l'immagine seguente. Potrete rimuovere il CD per fare l'avvio dall' hard disk. Adesso potete spegnere oppure riavviare il vostro computer.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksusper
) (aio/0) Done.
Waiting for processes to finish.......................................
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd) (
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.......................................
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/ini
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes]._
```

Attendere questo messaggio alla chiusura

15.3. Come posso eseguire una scansione antivirus?

Un assistente apparirà quando il processo di avvio sarà terminato e vi permetterà di eseguire una scansione completa del vostro computer. Tutto quello che dovete fare è cliccare sul tasto **Avvio**.

Nota
Se la risoluzione del vostro schermo non è abbastanza alta, vi verrà chiesto di cominciare la scansione in modalità di testo.

Seguire la procedura di tre passi per completare il processo di scansione.

1. Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

   Nota
   La durata del processo dipende dalla complessità della scansione.

2. Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

   I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

   Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.
3. E' possibile visualizzare il sommario dei risultati.

Se si vogliono esaminare solo alcune directory, fare come segue:

Sfogliare le vostre cartelle, fare un click con il tasto destro su un file o una directory e selezionare **Send to**. Quindi scegliere **BitDefender Scanner**.

Oppure potete emettere il comanso successivo come root, da un terminale. Il **BitDefender Antivirus Scanner** inizierà con il file o la cartella selezionati come ubicazioni predefinite dove eseguire la scansione.

```
# bdscan /path/to/scan/
```

15.4. Come posso salvare ai miei dati?

Supponiamo che non potete avviare il vostro PC Windows a causa di problemi sconosciuti. Nello stesso tempo, avete un bisogno disperato di accedere ad alcuni dati importanti sul vostro computer. Questo è il momento in cui BitDefender Rescue CD diventa utile.

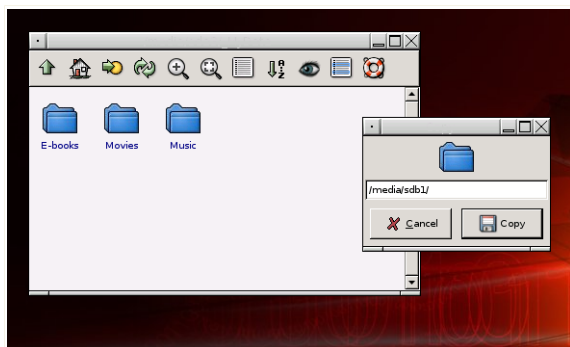
Per salvare i vostri dati dal computer ad un dispositivo rimuovibile, come una penna USB, basta seguire questi passaggi:

1. Inserire BitDefender Rescue CD nel lettore CD, la penna USB nella porta USB e quindi riavviare il computer.
2. Attendere finchè BitDefender Rescue CD completi l'avvio. Apparirà la seguente finestra.

Schermo del Desktop

3. Cliccare due volte sulla partizione dove sono ubicati i dati che volete salvare (e.g. `[sda3]`).

Nota
Quando lavorate con BitDefender Rescue CD, avrete a che fare con nomi di partizioni Linux. Quindi, `[sda1]` probabilmente corrisponderà alla partizione Windows `(C:)`, `[sda3]` alla `(F:)`, e `[sdb1]` alla penna USB.

4. Sfogliare le vostre cartelle ed aprire la directory desiderata. Per esempio, `MyData`, contenente le sottodirectory`Movies`, `Music` ed `E-books`.
5. Cliccare con il tasto destro sulla directory desiderata e selezionare **Copiare**. Apparirà la seguente finestra.

Salvataggio dei dati

6. Scrivere `/media/sdb1/` nella corrispondente casella di testo e cliccare **Copiare**.

Ottenere aiuto

16. Supporto

Come fornitore di valore, BitDefender si opera al massimo per offrire ai propri clienti un alto livello di supporto, veloce ed accurato. Il Centro di Supporto (che potete contattare all'indirizzo fornito di seguito) è in continuo aggiornamento con le ultime e nuove descrizioni dei virus. In questo modo avrete sempre una risposta puntuale alle vostre domande / richieste.

Con BitDefender, è considerata prioritaria l'ottimizzazione del tempo e della spesa necessari alla sicurezza degli utenti, con la fornitura dei prodotti più avanzati ai migliori prezzi. Inoltre crediamo che un business di successo sia basato in una buona comunicazione ed un impegno costante nel dare supporto all’utente.

Potete chiedere supporto in qualsiasi momento a support@bitdefender.com. Per una risposta veloce, vi chiediamo di includere nella vostra mail il maggior numero di dettagli possibile sul vostro BitDefender, sul sistema e di descrivere i problema con la maggior accuratezza possibile.

16.1. BitDefender Knowledge Base(Archivio di informazione BitDefender)

L’ Archivio di informazione BitDefender è un deposito di informazioni sui prodotti BitDefender. Immagazzina, in un formato facilmente accessibile, rapporti sui risultati del supporto tecnico in corso e attività di disinfezione dei team di supporto e sviluppo di BitDefender , insieme a più articoli sulla prevenzione dai virus, la gestione delle soluzioni BitDefender e spiegazioni dettagliate, oltre a molti altri articoli.

L'Archivio D’informazione BitDefender è aperto al pubblico e usufruibile gratuitamente. Questa ricchezza di informazioni è uno dei tanti modi di fornire ai clienti di BitDefender le conoscenze tecniche e la comprensione necessarie. Tutte le richieste valide di informazione o rapporti su difetti, provenienti da clienti di BitDefender trovano la loro esatta collocazione nell’Archivio di informazione BitDefender, come rapporti di disinfezione, i modi di aggirare le truffe, oppure gli articoli informativi, in modo di implementare i files di aiuto al prodotto.

L’ Archivio di informazione BitDefender è disponibile in qualsiasi momento all'indirizzo: http://kb.bitdefender.com.

16.2. Chiedere Aiuto

16.2.1. Vai al Web Fai-da-te

Avete una domanda? I nostri esperti di sicurezza sono disponibili per aiutarvi 24/7 al telefono, via e-mail o chat senza costi aggiuntivi.

Vi preghiamo di seguire i links sotto:

Inglese

BitDefender Total Security 2008
http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2193/

Tedesco

BitDefender Total Security 2008
http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2193/

Francese

BitDefender Total Security 2008
http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2193/

Romeno

BitDefender Total Security 2008
http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2193/

Spagnolo

BitDefender Total Security 2008
http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2193/

16.2.2. Aprire un ticket di supporto

Se desiderate aprire un ticket di supporto e ricevere aiuto via mail, utilizzare uno di questi link:

Inglese: http://www.bitdefender.com/site/Main/contact/1/

Tedesco: http://www.bitdefender.de/site/Main/contact/1/
Francese: http://www.bitdefender.fr/site/Main/contact/1/
Romeno: http://www.bitdefender.ro/site/Main/contact/1/
Spagnolo: http://www.bitdefender.es/site/Main/contact/1/

16.3. Contatti

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 10 anni BITDEFENDER ha acquisito una reputazione inestimabile superando le aspettative di clienti e partners, sforzandosi costantemente per una comunicazione sempre più efficiente. Se avete delle domande o richieste, non esitare a contattarci.

16.3.1. Indirizzi Web

Dipartimento vendite: sales@bitdefender.com
Supporto tecnico: support@bitdefender.com
Documentazione: documentation@bitdefender.com
Programma Partner: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Rapporti con i Media: pr@bitdefender.com
Opportunità di lavoro: jobs@bitdefender.com
Invio Virus: virus_submission@bitdefender.com
Invio Spam: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Pagina web prodotto: http://www.bitdefender.com
Archivi ftp del prodotto: ftp://ftp.bitdefender.com/pub
Distributori locali: http://www.bitdefender.com/partner_list
Archivio di Informazione BitDefender: http://kb.bitdefender.com

16.3.2. Uffici di Filiale

Gli uffici di BitDefender sono pronti a rispondere a qualunque richiesta relativamente alle loro aree di operazione, sia in materia commerciale che generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

Germany

BitDefender GmbH
Quartier generale Europa Occidentale
Karlsdorferstrasse 56

88069 Tettnang
Germany
Tel: +49 7542 9444 60
Fax: +49 7542 9444 99
E-mail: info@bitdefender.com
Vendite: sales@bitdefender.com
Web: http://www.bitdefender.com
Supporto tecnico: support@bitdefender.com

Italy

Shaft Srl
Torino
Supporto tecnico: support@bitdefender.com
Vendite: sales@bitdefender.com
Tel: +39 011 659 60 87
Fax: +39 011 833 86 59
http://www.bitdefender.com/it/Main/view/Prices_home.html

Glossario

ActiveX

ActiveX è una modalità di scrittura di Programmi che possano essere richiamati da altri Programmi e sistemi operativi. La tecnologia ActiveX è utilizzata con Microsoft Internet Explorer per generare pagine Web interattive che appaiano e si comportino come applicazioni invece che come pagine statiche. Con ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare pulsanti ed interagire in altri modi con la pagina Web. I controlli ActiveX sono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

L' adware è spesso combinato con un' applicazione host che è offerta senza spese quando l'utente accetta l'adware. Considerando che applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove viene spiegato il proposito dell' applicazione, non viene commessa alcuna infrazione.

Comunque, i pop-up di avvertimento possono diventare un fastidio, ed in alcuni casi riduce le performance del sistema. Inoltre, l'informazione che viene raccolta da queste applicazioni può causare inconvenienti riguardo la privacy degli utenti non sempre completamente informati sui termini dell'accordo di licenza.

Archivio

Disco, nastro o cartella che contiene files memorizzati.

Un file che contiene uno o più files in forma compressa.

Backdoor

Breccia nella sicurezza di un sistema deliberatamente lasciata dal programmatore o dal manutentore. La presenza di tali “brecce” non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del produttore a scopo di manutenzione.

Settore di Boot

Settore all'inizio di ogni disco che ne identifica l'architettura (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Virus di Boot

Virus che infetta il settore di boot di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infetto con un virus di boot, farà sì che il virus venga attivato nella memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.

Browser

Abbreviazione di Web browser, un'applicazione software utilizzata per localizzare e visualizzare pagine Web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono Browser grafici, ovvero in grado di visualizzare sia la grafica che il testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, inclusi suoni e animazioni, nonostante richiedano i plug-in per alcuni formati.

Linea di Comando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di comando.

Cookie

Nell'industria di Internet, i cookies vengono descritti come piccoli files contenenti informazioni relative ai computers individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia dei vostri interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire direttamente ciò che si dichiara essere di proprio interesse. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Dall'altra parte, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. In considerazione di questo è in atto un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un " SKU number" (il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Disk drive

È un dispositivo che legge e scrive dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy ospita i flpopy disks.

I drive di disco possono essere sia interni (incorporati all'interno di un computer) che esterni (collocati in un meccanismo separato e connesso al computer).

Download

Per copiare dati (solitamente un file intero) da un'origine principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio on-line sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

E-mail

Posta elettronica. Servizio che invia messaggi ai computers attraverso reti locali o globali.

Eventi

Azione oppure evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come un click con il mouse o premere un tasto sulla tastiera oppure accadimenti del sistema, come l'esaurimento della memoria.

Falso positivo

Si verifica quando una scansione individua un file come come infetto quando di fatto non lo è.

Estensione del nome di un file

La porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: “c” per codici fonte C, “ps” per PostScipt, “txt” per testi arbitrari.

Euristico

Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche impronte dei virus. Il vantaggio della scansione euristica è di non venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Applet Java

Programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisognerà specificare il nome dell'applet e la dimensione (lunghezza e larghezza -in pixel) che può utilizzare. Quando si accede

alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli Applets differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, nonostante gli applets vengano lanciati sul client, non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applets sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Macro virus

Tipo di virus del computer che è codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il questo viene aperto.

Client mail

La client e-mail è un'applicazione che vi consente di inviare e ricevere e-mail.

Memoria

Aree di immagazzinaggio interne al computer. Il termine memoria identifica l'immagazzinaggio dati sotto forma di chip; la parola storage viene utilizzata per la memoria su nastri o su dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

Non euristico

Questo metodo di scansione si basa su specifiche impronte di virus. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare un virus e non genera falsi allarmi.

Programmi impaccati

File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che impacca i files potrebbe sostituire gli spazi dei caratteri con un carattere speciale space_series seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.

Percorso

I percorsi esatti per raggiungere un file su un computer. Questi percorsi vengono solitamente descritti attraverso il sistema di casellario gerarchico dall'alto al basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazione tra due computer.

Phishing

L'atto d'inviare una mail ad un utente fingendo di essere una ditta legittima ed affermata, nel tentativo di truffare l'utente, facendogli cedere informazione private che verranno usati per furti d'identità. La e-mail indirizza gli utenti a visitare una pagina Web, dove viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto in banca. In ogni caso, la pagina Web è falsa e organizzata soltanto per rubare le informazioni dell' utente.

Virus Polimorfico

Virus che modifica la propria forma da ogni file che infetta. Non disponendo di caratteristiche binarie costanti, questi virus sono difficili da identificare.

Porta

Interfaccia su un computer dalla quale è possibile connettere un supporto. I Personal Computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitors e tastiere. Esternamente i Personal Computer hanno porte per la connessione dei modems, delle stampanti, del mouse e altri supporti periferici.

Nelle reti TCP/IP e UDP, un punto di arrivo ad una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

File di report

File che elenca le azioni avvenute. BitDefender mantiene un file di report che elenca i percorsi esaminati, le cartelle, il numero di archivi, i file esaminati, quanti file infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore ad un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la loro presenza in modo da non dover essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono maligni per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file crirtici utilizzando rootkit. Comunque, essi vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati al malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e log ed evitare il rilevamento.

Script

Altro termine per macro o bat ch file, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiai e-mail non richiesta.

Spyware

Qualsiasi software che accede alla connessione internet dell'utente senza che questo se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware arrivano tipicamente come un componente nascosto di programmi freeware o shareware che possono essere scaricati da Internet. Tuttavia, deve essere segnalato che la maggioranza delle applicazioni shareware o freeware non arrivano con spyware. Una volta installato, lo spyware esegue il monitoraggio dell'attività dell' utente su Internet e trasmette questa informazione di nascosto a qualcun altro. Lo spyware può anche raccogliere informazioni su indirizzi mail e addirittura passwords e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano inconsapevolmente installando applicazioni diverse. Un modo comune per diventare vittima dello spyware è scaricare alcuni files peer-to-peer scambiando prodotti che sono disponibili oggi.

Non rispettando l'etica e la privacy, lo spyware approfitta dell' utente usando risorse di memoria del computer "assorbendo" larghezza di banda dal momento in cui invia informazioni alla sua "base" utilizzando la connessione internet dell' utente. Dato che lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in sottofondo (background) possono portare alla caduta del sistema o alla sua instabilità.

Elementi di startup

Qualsiasi file posizionato in questa cartella si aprirà quando il computer sarà avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il file stesso.

Barra di sistema

Introdotta con Windows 95, la barra di sistema è situata nella barra strumenti di Windows (solitamente in basso vicino all'orologio) e contiene icone miniaturizzate per un semplice accesso alle funzioni di sistema, come ad esempio il fax, la stampante, il modem, il volume ed altro. Fare doppio click o fare click con il tasto destro su un'icona per vedere ed accedere ai dettagli ed ai controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di networking largamente utilizzati su Internet che consentono le comunicazioni attraverso le reti interconnesse di computers con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computers e le convenzioni per connettere le reti e il traffico di instradamento.

Trojan

Programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus del vostro computer ma che al contrario li introduce.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e catturare Troia.

Aggiornamento

La nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul vostro computer; diversamente non sarà possibile installare l'aggiornamento.

BitDefender dispone del proprio modulo che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Virus

Programma o parte di codice caricato sul vostro computer a vostra insaputa e che viene eseguito contro la vostra volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus del computer sono creati dall'uomo. E' relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Definizione di virus

Caratteristica binaria di un virus, utilizzata dal programma antivirus al fine di rilevare ed eliminare il virus stesso.

Worm(baco)

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.